UNITED STATES DEPARTMENT OF AGRICULTURE
AGRICULTURAL MARKETING SERVICE

DIRECTIVE

3130.11 **5/29/2007**

PROTECTING SENSITIVE INFORMATION

I. POLICY

It is the responsibility of all AMS employees to protect all sensitive information from unauthorized disclosure in order to protect the identities of employees and the public, as well as to safeguard the public's confidence in the Agency's mission delivery. Sensitive information is to be collected, stored, and used by AMS programs only when absolutely necessary for the conduct of official business.

II. WHAT IS SENSITIVE INFORMATION?

Sensitive information can be either:

A. Personally Identifying Information. This is information used to distinguish or trace an individual's identity, such as Social Security number, home address, personal telephone number, sex, date of birth, place of birth, financial facts, or medical facts that are associated with the name of an individual. This information is also referred to as Privacy Act information.

B. Sensitive But Unclassified Information. This is any information not for public distribution such as Continuity of Operations Plans (COOP), cyber-security plans, budget reports, preliminary rule-making documents, or documents such as grading certificates that contain proprietary company information.

III. HOW SHOULD SENSITIVE INFORMATION BE PROTECTED?

A. Eliminate sensitive information that is not essential for program operation. Whenever possible, do not collect, store, or use sensitive information unless its use is required by law or regulation, or its use is absolutely essential for your program operation.

B. Establish effective controls in accordance with risk. When sensitive information must be used, controls over that information will vary depending on where the information is used. Whenever possible, sensitive information should be kept and used only within USDA office space. In cases where its use outside of USDA office space is essential for the delivery of services, additional controls are necessary to offset the greater risk of unauthorized access.

IV. WHAT CONTROLS SHOULD BE USED WITHIN USDA OFFICE SPACE?

A. Electronic files such as spreadsheets, word processing documents, and Access database files that are stored on a personal computer and contain sensitive information shall be encrypted through the use of the Microsoft Encrypting File System (EFS).

B. Electronic databases such as SQL Server and Oracle databases that are stored on a file server and contain sensitive information shall:

1. Be protected by controls that ensure the sensitive data is accessed and used only by those users with a valid business need; and

2. Have the fields containing sensitive information or the entire database encrypted whenever possible with the strongest means available to prevent unauthorized users from being able to read the content of a database copy.

C. Printed materials that contain sensitive information shall be:

1. Conspicuously labeled as "Sensitive Information" or "For Official Use Only" and whenever possible contain the additional statement "Protect from Unauthorized Disclosure."

2. Protected by administrative access controls that ensure it is accessed and used only by those users with a valid business need. Such controls should address how the material is stored when not in use, how it is protected when it is in use, who may use the material, and how the material is destroyed when it is obsolete.

3. Protected by administrative access controls that ensure any copies made of the report are also known and subject to the same controls as the original copy.

4. Stored during non-duty hours in a locked desk, file cabinet, room, or storage area with appropriate access controls that would prevent unauthorized access.

V. WHAT CONTROLS SHOULD BE USED OUTSIDE USDA OFFICE SPACE?

All controls used for protecting sensitive information within USDA office space apply to sensitive information used outside of USDA office space. In addition, the following actions shall also apply:

A. Electronic files containing sensitive information that are stored on a laptop, personal computer, personal digital assistant (PDA), or removable storage device shall be:

1. Part of an established information system where the use of the sensitive information and related controls is documented by an accurate Privacy Impact Assessment on file with the Agency Cyber-Security Branch;

2. Encrypted through the use of the Microsoft Encrypting File System (EFS) or other device appropriate encryption protection (contact your system administrator or the AMS Help Desk for assistance with EFS);

3. Stored ONLY on Government computers and devices and NEVER on personally-owned computers and devices;

4. Approved for remote use by the supervisor; and

5. Protected using every reasonable precaution to minimize the probability that the device that contains the files could be stolen. Typically, this will require that the responsible official maintain the highest level of control and awareness over the device that is reasonably possible.

B. Printed materials that contain sensitive information and are used outside of USDA office space shall be:

1. Part of an established system where the use of the sensitive information and related controls is documented by an accurate Privacy Impact Assessment on file with the Agency Cyber-Security Branch;

2. Approved for remote use by the supervisor; and

3. Protected using every reasonable precaution to minimize the probability that the document could be viewed by unauthorized individuals, copied, or stolen. Typically, this will require that the responsible official maintain the highest level of control and awareness over the material that is reasonably possible.

VI. WHAT ACTION SHOULD BE TAKEN WHEN UNAUTHORIZED ACCESS OCCURS?

A. What should I do if I reasonably suspect or know that unauthorized access to sensitive electronic or printed information has occurred?

1. *Immediately* contact your supervisor and your program's lead system administrator. Prompt reporting is required to allow the Agency to respond in a timely fashion to mitigate any damage to individuals or the Agency program.

2. When the access involves personally identifiable information, program system administrators will immediately report the incident to the Agency CyberSecurity Branch Chief or Chief Information Officer so that the Agency can report the incident to the Department within one hour of notification. The Department in turn will notify US CERT, a unit of the Department of Homeland Security, and the USDA Office of the Inspector General.

B. What should I do if I reasonably suspect or know that Government-issued information technology equipment such as a laptop, computer, blackberry, or removable media has been lost or stolen?

1. *Immediately* contact your supervisor. Then either you or your supervisor should call the hotline number below:

TOLL FREE LOST AND STOLEN EQUIPMENT HOTLINE: 1-888-926-2373

Be prepared to answer questions about the incident, including:

- Who, what, when, and where
- What type of information was stored on the equipment, and
- Specifically, if sensitive information was stored on the equipment.

After calling the hotline, contact your program's lead system administrator and advise them of the loss and the actions you have taken. Additionally, if sensitive information was stored on the lost or stolen equipment, be certain that the instructions above are followed for reporting unauthorized access to sensitive information.

/s/

Lloyd C. Day
Administrator