United States Department of Agriculture
Grain Inspection, Packers and Stockyards Administration

Directive GIPSA 3140.2 1/30/01

GIPSA MICROCOMPUTER, LOCAL AREA NETWORK (LAN), AND NOTEBOOK COMPUTER POLICY

1. PURPOSE

This Directive establishes policy and provides information on securing the Grain Inspection, Packers and Stockyards Administration's (GIPSA) computer hardware, software, and data. Each user is to be aware of the basic security measures and implement them in the daily use of microcomputers and related components.

2. REPLACEMENT HIGHLIGHTS

This Directive updates Directive 3140.2, dated November 15, 1999, due to changes in technology and the need to provide guidance for these new technologies; specifically, the Internet and web-based technology.

3. AUTHORITIES/REFERENCES

a. Computer Fraud and Abuse Act. All Government computers are subject to the Computer Fraud and Abuse Act of 1984 (Pub. L. 98473) and its 1986 revision (Pub. L. 99-474). This act provides for punishment of individuals who commit fraud on or abuse Government computers. To comply with these laws and allow prosecution of offenders, Department Manual (DM) 3140-1, USDA, ADP Security Manual, Appendix J requires that all users be warned that it is unlawful to use any Government computer for unauthorized purposes. Specifically, use of a government computer "without authorization or for purposes for which authorization has not been extended is a violation of Federal Law and can be punished with fines or imprisonment (P.L. 99-474)." Report suspected violations to your Supervisor, Security Representative or ISSPM.
GIPSA employees can send anonymous letters to any of the above.

b. Computer Security Act of 1987. The Computer Security Act of 1987 (Pub. L. 100-235):

(1) Provides for Government-wide computer security, and

(2) Declares "that improving the security and privacy of sensitive information in Federal computer systems is in the public interest." The Act defines sensitive information as "… any information, the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept in the national interest of national defense or foreign policy."

DM 3140-1, defines sensitive information as "…information loss, unauthorized modification, unauthorized disclosure would be detrimental to Agency operations. Examples: information that is personal, proprietary, financial, National-security related, or critical to Agency plans and operations."

USDA Internet Security Policy, This regulation establishes minimum-security requirements for the use of the Internet network by USDA employees.

c. GIPSA further defines sensitive information to include:

(1) Information that is prohibited from disclosure under the Freedom of Information Act.

(2) Proprietary information and software.

(3) Copyright-protected software and manuals.

(4) Disciplinary actions and other "need to know" personnel related information.

(5) Whistleblower complaints.

(6) Audit reports

(7) Investigation reports

(8) Civil and criminal violations.

(9) Information subject to signed nondisclosure forms.

(10) Strategic plans until released.

(11) Security and contingency plans.

(12) Programs, data, or information that can be used for financial gain.

(13) EEO and civil rights cases and issues.

(14) Highly sensitive budgetary information that has not been released by the President.

d. For Official Use Only (FOUO). DM 3440-1 defines FOUO information as "…an administrative marking applied to official information which requires protection in accordance with statutory requirements or in the public interest, but which is not within the purview of the rules for safeguarding information in the interest of national security. GIPSA FOUO information will be protected from unauthorized disclosure, transmission or release until authorization is granted for its release.

FOUO information will:

(1) Not be stored on LAN servers, unless specific protections are in place to prevent unauthorized access.

(2) Be removed from unsecured microcomputers and the media stored in locked safes, file cabinets, or desks with keys controlled by those authorized to handle this information.
Use the same protection procedure to store backup copies of FOUO information.

4. POLICY

a. Microcomputer Security

(1) All offices are to implement and maintain physical security measures to ensure the physical and electronic protection of hardware, software, and data.

(a) Office doors should be locked at night. Offices should also be locked when leaving for lengthy meetings or seminars.

(b) Log off the network when office/microcomputer is unattended. All microcomputers should be powered off when leaving for the day.

(c) Enable screensaver passwords for microcomputers.
Use the screensaver's that are shipped with the operating system. Do not download screensavers from the internet.

(d) Secure any media (floppy disks, backup tapes) that contain sensitive data.

(2) Backups must be performed on a regular basis. Each GIPSA employee is responsible for his/her own data. If a GIPSA employee has access to a LAN, then ALL data must be stored on the LAN. No data is to be stored on the local microcomputer hard drive when the system has a LAN connection.

(3) All application software and documentation of production systems, along with backups of critical data, must be stored in a location away from the computer.
Application software refers to off the shelf software such as Microsoft Office, Norton Anti-virus, Reflection etc.
Production systems are those programs create by GIPSA for GIPSA use.

(4) All GIPSA computers and equipment are to be used for official purposes only. The only exceptions are “limited use” for e-mail and Internet uses.

(5) All microcomputers and peripherals are to be equipped with power strip/surge suppressors. Microcomputers used as servers must have a un-interruptible power supply (UPS) with at least 30 minutes of battery supplied power available.

(6) SMOKING, DRINKING, and EATING in the immediate vicinity of any microcomputer is discouraged. Food particles that are dropped on the keyboard can work down around the keys and cause them to malfunction. Any liquids spilled on the hardware or storage media can cause irreparable damage.

(7) If any sensitive or confidential information is stored on the hard drive of any microcomputer or notebook computer, security should be implemented such that a password must be entered before access to any device on the computer is enabled. Any microcomputer with a LAN connection must store all data on the server.

b. Software and Data Security.

(1) All passwords are to be kept confidential and changed on a regular basis. Passwords must be a minimum of 8 alpha/numeric characters and changed at least every 90 days for network/e-mail accounts and 180 days for batch applications. Since passwords are used as keys to critical data and systems, they should be protected. Do not give out your password for others to use. Passwords must

not be posted on the computer terminal, bulletin boards, partitions, walls, etc. The best practice is for the user to seal passwords in an envelope and lock them in a secure place.

(2) All microcomputer and LAN software purchased by, or licensed to, GIPSA is automatically protected by Federal copyright law. Copying, duplicating, or selling copyrighted material without a written release is strictly prohibited.

(3) It is illegal to load or install on GIPSA microcomputers and LAN's copyrighted software that was purchased by others and licensed on non-GIPSA microcomputers, unless written permission has been obtained from the license owner and the Information Systems Security Program Manager (ISSPM).
Installation of software obtained in violation of copyright restrictions on any GIPSA microcomputer is prohibited.

(4) Non-standard Agency software will not be installed without written permission from the Supervisor of the Information Technology (IT) group responsible for the PC.

The Supervisor of the IT group can make exceptions for Field Office Computer Specialists/System Administrator's with regards to applying updates and peripheral drivers (printers, scanners, etc.) This exception is up to the IT Supervisor.

(5) Removing GIPSA-purchased or GIPSA-licensed software from any Government computer, LAN, office, or building for purposes other than approved official business is prohibited.

(6) Software given to GIPSA employees by vendors or trainers at GIPSA-funded training, conferences, seminars, or expositions becomes the property of GIPSA. It may be used by employees on their GIPSA microcomputers when it complies with the following conditions:

(a) Written permission has been obtained from the Supervisor of the Information Technology (IT) group responsible for the PC.

(b) It is scanned for viruses before installing or using;

(c) It does not conflict with standard GIPSA software;

(d) It is installed or used according to documentation accompanying the diskette compact disk; and

Non copyright-protected software, such as Freeware, Shareware, or demonstration software, will not be copied, installed, or loaded onto a GIPSA microcomputer or LAN without the written permission from the Supervisor of the Information Technology (IT) group responsible for the PC.
GIPSA will not provide support for this software.

(7) Removing GIPSA-purchased, copyright-protected software from any GIPSA microcomputer or LAN without written authorization is prohibited. Obsolete or outdated copyright-protected software that has been replaced by a newer version will be returned to the Security Representative in Field locations and to the IT Staff in D.C./TSD for disposition. Obsolete or outdated copy-protected software must be handled in compliance with instructions accompanying upgrade software, or as specified in the copyright agreement accompanying the software. Under no circumstances will earlier versions of software be diverted to personal or private use. Each of GIPSA's IT groups will maintain an inventory of all authorized software in their area.

(8) U.S. Department of Agriculture (USDA) regulations require all USDA agencies to acquire and use microcomputer anti-virus software on all microcomputers.
GIPSA employees are solely responsible for vigilance concerning viruses, worms and other malicious code.
GIPSA-purchased or -supplied anti-virus software will be activated and executed to check for malicious microcomputer software on media, files, and memory each time a GIPSA microcomputer is turned on.
The following also will be scanned for microcomputer viruses:

(a) All incoming/outgoing microcomputer, LAN and e-mail files.

(b) All approved software and information downloaded from the Internet or received by modem on microcomputer or LAN; and

(c) All media received in official training that was conducted using non-GIPSA computers.

(9) Electronic mail will be used for official government business only except for the provisions outlined in Departmental Regulation 3300-1 (DR 3300-1), Telecommunications & Internet Services and Use, section entitled Approval of Limited Personal Use Policy.

(10) All data files, i.e. correspondence, spreadsheets, database files, etc., should be stored on the network to ensure that they are secured and backed up. If information is stored on the hard drive of any microcomputer, these systems must also be backed up individually. It is up to each GIPSA employee to be responsible for his/her data back-ups.

c. Document Retention; Disposal of Documents, Software, and Hardware

(1) Any document that is produced from a GIPSA system or any system that the agency utilizes (e.g. accounting, personnel, etc.) containing sensitive or confidential data should be properly stored in a locked file cabinet, desk, or other secure container.

(2) Any document containing sensitive or confidential data that is to be disposed of should be according to Agency established records management requirements.

(3) Any microcomputer or server that is to be disposed of or donated to a school should be done so only after the hard drive has been cleared of all software and Agency related data.

(4) All diskettes or tapes with sensitive or confidential data will be disposed according Agency established records management requirements.

(5) All commercial software diskettes that are to be disposed of will be destroyed before dismissal.

d. Local Area Network (LAN) Security:

Of the general requirements for information technology to effectively meet its business objectives, the following three are necessary for effective security: Confidentiality, Integrity, and Availability.

Confidentiality - Protecting information from unauthorized disclosure. The system should be designed and implemented to ensure the optimum control over computer data and program files. Privacy, sensitivity, and secrecy are issues here.

Integrity - Provide adequate protection from unauthorized, unanticipated or unintentional modification ensuring data is accurate and complete, including:

(1) Ensuring consistency of data values within a computer system;

(2) Recovering to a known consistent state in the event of a system failure;

(3) Ensuring that data is modified only in authorized ways; and

(4) Maintaining consistency between information internal to the computer system and the realities of the outside world.

Availability - Information must be available on a timely basis wherever it is needed to meet business requirements or to avoid substantial losses. Uninterrupted access to information and system resources, such as data, program and equipment, is a fundamental need.

e. Sensitive Information - The Computer Security Act defines sensitive information as "any information the loss, misuse or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5 United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." By this definition, a system is considered sensitive if it meets the conditions of confidentiality, integrity or availability.

(1) Data Back-up

(a) Full backups and/or incremental are performed nightly on all GIPSA minicomputer and LAN microcomputer servers. Individual computers not on the LAN will do their own backups.

(b) A complete backup is stored at a secure off-site location once a month. This off-site storage is for catastrophic recovery and should not be in close proximity to the operational site.

(c) Backup procedures are documented, a backup log is kept, and all backup tapes are clearly labeled.

(2) Data Integrity

(a) Access to all GIPSA LAN servers/minicomputers is to be password protected. If possible, access to stand alone PC's should be password protected.

(b) Anti-virus software runs, at a minimum, once daily on each server.

(c) Anti-virus software is kept updated.

(d) Servers are to be monitored daily for unusual activity, excessive after hours use, unsuccessful password attempts, unusual out dialing patterns, and unexplained reduction in storage capacity.
Keep system logs to monitor network activity.

(e) Request identification from service equipment vendors and technicians.

(f) A member of GIPSA's IT staff must remain in server room while service equipment vendor or technician is present. Outside contractors will never be left alone in any GIPSA server facility.

(3) Physical Security

The following are minimum requirements. Physical security for server/computer rooms must be commensurate with the security level of the data being protected. For details, see DM 3140-1.2

(a) All Local Area Network (LAN) file servers are to be equipped with an un-interruptible power supply (UPS) with at least 30 minutes of battery supplied power available.

(b) All minicomputer and LAN file servers are to be secured in a separate room from the general office area. This room is to have an "panic" off switch located at the room exit.

(c) All server rooms are to have a cipher lock installed. Combinations to these locks will only be given to responsible GIPSA IT staff. Secure location of network servers when unattended.

(d) All GIPSA servers must have a surge/spike protector installed.

(e) Adequate heating and cooling controls are to be in place.

(f) Smoke detectors must be installed.

(g) Fire extinguisher located in server room.
Personnel must be familiar with the use of fire extinguisher.

(h) Personnel must be knowledgeable on their responsibilities in case of fire or natural disaster. These responsibilities are outlined in the Occupant Emergency Plan (OEP).

4. AUTHORITIES/REFERENCES

a. Computer Fraud and Abuse Act. All Government computers are subject to the Computer Fraud and Abuse Act of 1984 (Pub. L. 98473) and its 1986 revision (Pub. L. 99-474). This Act provides for punishment of individuals who commit fraud on or abuse Government computers. To comply with these laws and allow prosecution of offenders, Department Manual (DM) 3140-1, USDA ADP Security Manual, Appendix J requires that all users be warned that it is unlawful to use any Government computer for unauthorized purposes. Specifically, use of a government computer "without authorization or for purposes for which authorization has not been extended is a violation of Federal Law and can be punished with fines or imprisonment (P.L. 99-474)." Report suspected violations to your Supervisor.

b. Computer Security Act of 1987. The Computer Security Act of 1987 (Pub. L. 100-235):

(1) Provides for Government-wide computer security, and

(2) Declares "that improving the security and privacy of sensitive information in Federal computer systems is in the public interest." The Act defines sensitive information as "… any information, the loss, misuse, or unauthorized access to, or modification of, which could **adversely affect** the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the national interest of national defense or foreign policy."

DM3140-1, defines sensitive information as " . . . information whose loss, unauthorized modification, unauthorized disclosure would be detrimental to Agency operations. Examples: information that is personal, proprietary, financial, National-security related, or critical to Agency plans and operations."

USDA Internet Security Policy. This regulation establishes minimum-security requirements for the use of the Internet network by USDA employees.

c. GIPSA further defines sensitive information to include:

(1) Information that is prohibited from disclosure under the Freedom of Information Act

(2) Proprietary information and software

(3) Copyright-protected software and manuals

(4) Disciplinary actions and other "need to know" personnel related information

(5) Whistleblower complaints

(6) Audit reports

(7) Investigation reports

(8) Civil and criminal violations

(9) Information subject to signed nondisclosure forms

(10) Strategic plans until released

(11) Security and contingency plans

(12) Programs, data, or information that can be used for financial gain

(13) EEO and civil rights cases and issues

(14) Highly sensitive budgetary information that has not been released by the President.

d. For Official Use Only (FOUO). DM 3440-1 defines FOUO information as " . . . an administrative marking applied to official information which requires protection in accordance with statutory requirements or in the public interest, but which is not within the purview of the rules for safeguarding information in the interest of national security. GIPSA FOUO information will be protected from unauthorized disclosure, transmission, or release until authorization is granted for its release.

FOUO information will:

(1) Not be stored on LAN servers, unless specific protections are in place to prevent unauthorized access.

(2) Be removed from unsecured microcomputers and the media stored

in locked safes, file cabinets, or desks with keys controlled by those authorized to handle this information.
Use the same protection procedure to store backup copies of FOUO information.

5. PROHIBITED PRACTICES, PRODUCTS, AND USES

The Standards of Ethical Conduct for Employees of the Executive Branch states: "Employees are prohibited from directly or indirectly using, or allowing the use of, Government property, facilities, or services of any kind, including those leased to or otherwise paid for by the Government, for other than officially approved activities. Employees have a positive duty to conserve and protect Government property."

Playing games on GIPSA microcomputers and LAN servers is prohibited. The prohibition includes installing and using software that is for personal use or private financial gain. The following are examples of prohibited software: Mortgage amortization software, personal checkbook software, private business packages, and income tax preparation packages, etc.

Installing, copying, displaying, demonstrating, or using sexually explicit material, such as nude calendars or pornographics, is **strictly prohibited** from GIPSA microcomputers and LAN's. Jokes, cartoons, violent and racially or ethnically insulting or demeaning messages, documents, sounds (.wav files) or graphics are included in the prohibition.

Strictly prohibited practices also include accessing or downloading ANY pornographic material via the Internet.

All of the prohibited items and media that are in any GIPSA office, GIPSA-funded project, or GIPSA-supplied microcomputers before receiving this policy will be removed immediately.

These prohibitions are in effect during normal duty hours, overtime, lunch periods, weekends, and holidays.

GIPSA employees will not attempt to access information not authorized to them because of their position.

6. PERMITTED PRACTICES

Employees may use GIPSA microcomputers to support their National Guard and Military Reserve duties and to prepare assignments required to successfully complete GIPSA-funded training, as long as those activities are official to the Guard or Reserves; not in conflict with GIPSA duties; not, in any way, violating or conflicting with this policy; and approved by the employee's supervisor.

7. FAX BOARDS/MACHINES

FAX boards will be used for official business only. The transmission of sensitive GIPSA information by FAX transmission is discouraged. FAX transmissions are subject to misrouting, garbling, and interception. Users are advised that FAX equipment is subject to unsolicited transmissions (junk FAX). It is illegal to solicit Federal employees while they are at work. Notify your office or ISSPM of any unsolicited messages.

8. PROTECTING ACCESS TO MODEMS

GIPSA microcomputer users and LAN managers need to be aware of the threats to copyright protected software and sensitive information from hackers, borrowers, and inadvertent access. Modems should not be left unattended in "autoanswer mode" without having security procedures in place to verify the caller's identity. GIPSA modems will not be used for attempting or completing unauthorized accesses, such as hacking. Modems that are no longer needed must be removed from the PC.

9. NOTEBOOK COMPUTERS AND PERSONAL DIGITAL ASSISTANTS (PDA’s)

a. Physical Protection

(1) To prevent physical damage or theft, use a sturdy, weatherproof, padded, adequately sized conservative bag which doesn't necessarily look like a computer bag.

(2) Use a locking device which will secure a notebook to a desk, table, etc.

(3) Do not leave notebook unattended, particularly overnight on desktops. If notebook is located in a high traffic area, use a notebook locking device. Secure notebook anytime it is unattended.

(4) Do not position notebook near exterior windows where they are subject to a smash and grab type theft.

(5) Airports:

(a) Never leave equipment unattended or out of sight.

(b) Never check a notebook as baggage.

(c) Let the notebook go through x-ray, never ask for hand inspection.

(d) As the notebook goes through x-ray, keep your eyes on it.

(e) If security wants to see it operate, you handle it. Try to never let them touch the computer.

(6) Storage in cars:

(a) If a notebook must be left in a car keep it locked and out of sight.

(b) While riding, place the case between the drivers seat and the rear seat so it won't slide around.

(c) Avoid storage in very cold or very hot weather.

b. Data Protection

(1) Backup files and keep current copies readily accessible.

(2) Use password locking programs.

(3) Use encryption programs or file compression with encryption programs.

(4) Do not use any “short-cut” programs or script files that could allow direct access into any GIPSA system.

(5) Do not store phone numbers to any GIPSA system on Notebook computers or PDA’s.

(6) Keep anti-viral software and virus signatures current.

(7) Keep a copy of the following information at office location: *(separate from the notebook computer)*

(a) Serial number of notebook.

(b) Current inventory of all software installed.

(c) ALL system account names your have access to.

c. Notebook loss or theft:

(1) Contact Security Representative (Field Office) or ISSPM (DC) immediately.

(2) Have the inventory information available for Security Representative or ISSPM.

10. INQUIRIES

Direct inquiries or requests for changes to this policy to the GIPSA ISSPM at (202) 690-0044.

Copies of current GISPA directives can be accessed on the Intranet site, “InGIPSA” and on the Internet at **www.aphis.usda.gov/library**.

/s/ David R. Shipman
Acting Administrator
GIPSA