




July 3, 2003

MEMORANDUM FOR HEADS OF SERVICES AND STAFF OFFICES
AND REGIONAL ADMINISTRATORS

FROM:  MICHAEL W. CARLETON
CHIEF INFORMATION OFFICER (I)

SUBJECT: GSA Information Technology (IT) General Rules of Behavior

This memorandum transmits the Order, "GSA Information Technology (IT) General Rules of Behavior," CIO 2104.1. GSA Instructional Letter CIO IL-02-02 is hereby cancelled. The purpose of this Order is to present a set of General Rules of Behavior as part of a comprehensive program to provide complete information security. A good security posture supports the business purpose of our organization. These IT Security Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computers and the data they contain is an essential part of their jobs.

We appreciate your continued cooperation in assisting us to implement information technology improvements and standardization to provide more efficient IT capability for all GSA associates and a more secure IT environment. Should you have any questions regarding this matter, contact me on (202) 501-1000.

Attachments

GSA ORDER

SUBJECT: GSA Information Technology (IT) General Rules of Behavior

1. Purpose. This order sets forth General Services Administration's (GSA's) policy on IT General Rules of Behavior. The IT General Rules of Behavior are based on GSA policies and guidelines and Federal documents, including GSA Order CIO HB 2100.1A IT Security Policy; GSA Order CIO 2160.2 Electronic Messaging Policy; Office of Management and Budget (OMB) Circular A-130 Appendix III Management of Federal Information Resources; Federal Information Security Manager Act (FISMA) December 2002; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 An Introduction to Computer Security: the NIST Handbook; and NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.
2. Cancellation. Instructional Letter CIO IL-02-02 (July 3, 2002).
3. Objectives. The objectives of the IT General Rules of Behavior are to ensure that all authorized users of IT resources (i.e., computers, software, etc.) are aware of their responsibilities and expected behavior in safeguarding these resources.
4. Applicability. This order applies to all GSA Services, Staff Offices, and Regions, and to all GSA Federal employees and authorized users of GSA IT. Authorized users are associates of GSA and other Government organizations who are supported by GSA, and those contractors, consultants, or other third parties who are specifically granted access to conduct business on behalf of, or with, GSA or other Government organizations supported by GSA.
5. Roles and Responsibilities.
 - a. GSA Managers:
 - (1) Ensure that authorized users, including GSA associates and contractors, comply with this order.
 - (2) Ensure that GSA associates and contractors complete GSA's annual IT Security Awareness Training.
 - (3) Coordinate and arrange system access requests for all new or transferring employees and for verifying an individual's need-to-know (authorization)

b. Authorized Users of GSA IT Resources:

Must comply with the IT General Rules of Behavior.

c. GSA Designated Approving Authorities (DAAs):

(1) Ensure system/organization-unique rules be addressed as part of the overall risk management process for systems under the DAA's authority.

(2) Ensure that authorized users, including GSA associates and contractors, are provided these additional rules.

6. Penalties for Non-compliance. Users who do not comply with the IT General Rules of Behavior may incur disciplinary action and/or criminal prosecution.

7. General IT Rules of Behavior.

a. All GSA information resources, leased or owned, are the property of GSA. GSA's information resources are provided for GSA business purposes.

b. Users of GSA information system resources must use GSA information resources in an ethical and lawful manner and in accordance with this order.

c. Users of GSA information resources must use passwords that contain a minimum of 8 characters and a combination of letters, numbers, and special characters. GSA users are responsible for, and may be held accountable for, all accesses made with their userids/passwords. GSA users shall maintain the confidentiality of their passwords. At a minimum, this entails adhering to these guidelines:

(1) Do not share password with anyone including other associates, management, or technical personnel.

(2) Do not write, display, or store passwords where others may access or view them.

(3) Change passwords upon initial access to the system, and at least every 90 days as prompted.

(4) Immediately report to the appropriate Information Systems Security Officer (ISSO) any requests by others to reveal your password.

d. Users of GSA information resources must use up-to-date virus protection software on all systems accessing the GSA network.

e. Users shall complete annual IT security awareness training.

- f. Users shall report security incidents to their local helpdesk or ISSO.
- g. Users shall protect government property, resources and assets from theft, destruction, or misuse.
- h. Users shall not attempt unauthorized access of information contained in any system or application.
- i. Users must lock GSA systems with a password when away from the work area (e.g., for lunch, breaks or any extended period of time etc.).
- j. Users must logoff GSA systems at the end of the workday.

8. E-Mail and Internet Acceptable Use.

- a. Users should use E-mail for Government business. However, users may occasionally make personal use of E-Mail that involves minimal expense to the Government and does not interfere with Government business.
- b. Users must not use E-mail for any activity or purpose involving classified data.
- c. E-mail does not provide a secure means of sending sensitive and proprietary information outside of GSA. In such cases, encryption may be used but must be explicitly authorized by your DAA.
- d. Users shall not expect privacy on GSA IT systems. All activities on GSA IT systems are subject to monitoring.
- e. Users must avoid the following prohibited E-mail usages:
 - (1) Transmitting unsolicited commercial announcements or advertising material, unless approved by management in advance.
 - (2) Transmitting any material pertaining to GSA, the Federal Government, or any agency employee or official, that is slanderous or defamatory.
 - (3) Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, unauthorized mass mailings, or intentionally sending a virus/worm.

f. Personal use of Government resources to access the Internet shall be kept to a minimum and shall not interfere with official system use or access.

g. Prohibited Internet usages include:

- (1) Unauthorized attempts to break into any computer, whether belonging to GSA or another organization.
- (2) Browsing sexually explicit or hate-based web sites.
- (3) Using Internet access for personal gain (i.e. making use of GSA resources for commercial purposes or in support of for-profit activities such as running a private business).
- (4) Theft of copyrighted or otherwise legally protected material, including copying without permission.
- (5) Sending or posting non-encrypted material such as sensitive building drawings or financial information outside of the GSA network.

h. Detailed guidance regarding GSA E-Mail Policy is available in GSA Order CIO 2160.2, GSA Electronic Messaging Policy.

9. Remote Access Acceptable Use.

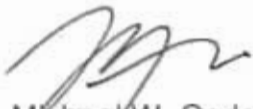
- a. Users shall not connect to other computers or networks via modem while simultaneously connected to the GSA network (e.g., no dialing outbound to your Internet Service Provider or allowing inbound calls to your computer while at the same time being connected to GSA's network). However, accessing GSA's network via the GSA-provided Virtual Private Network (VPN) software is allowed.
- b. Users shall treat GSA dial-up numbers as confidential and privileged information.

10. Software Acceptable Use.

- a. Users of GSA IT resources shall use only software that is properly licensed and registered for GSA use. All GSA users must abide by software copyright laws and shall not obtain, install, replicate, or use unlicensed software.
- b. Users of GSA IT resources must obtain all software from GSA sources and shall not download software from the Internet without prior permission from the appropriate ISSO, as downloading software from the Internet may introduce viruses/worms to the GSA network.

- c. Users shall not install any software or hardware without approval of the appropriate ISSO.
- d. Users shall not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise GSA resources unless authorized by the appropriate ISSO. Examples of such tools include those that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

11. Deviations. All deviations from this order shall be coordinated by the ISSO through their appropriate DAA. The DAA shall notify the GSA Senior Agency Information Security Official (SAISO) of any deviations.



Michael W. Carleton
Chief Information Officer