



Order

Subject: Use of Information Technology Resources

Directive Number: Part: IM Section: 05-04

Effective Date: 4/26/06 Originator: OIT

Chief Administrative Officer

1. **PURPOSE:** This directive establishes the use of PBGC information technology (IT) resources for official business and limited personal use. The personal use privilege is intended to be limited and should not be abused.
2. **SCOPE:** This directive applies to all PBGC Federal employees, bargaining-unit and non-bargaining-unit and contractors irrespective of how the staff member accesses IT resources, whether locally or remotely. Notwithstanding this policy, PBGC may take emergency action as necessary to protect these resources. Note: If deemed appropriate by PBGC management, any exceptions for union officers and stewards will be set forth in the applicable collective bargaining agreement or in a specific agreement between PBGC and the union.
3. **AUTHORITIES:**
Clinger-Cohen Act of 1996
Executive Order 13011, Federal Information Technology
Standards of Conduct of the Executive Branch
OMB Circular A-130, Appendix III(3)(a)(b)
OMB Memorandum for Chief Information Officers, September 8, 2004
4. **BACKGROUND:** PBGC policy is needed to ensure that the IT resources are available for official business as necessary by limiting personal (non-official) use, taking actions necessary to protect its resources, including responding to any threats, and ensuring that its computer and telephone networks are stable.

All staff members have an obligation to protect and conserve U.S. Government property as well as an ethical obligation to perform an honest day's work both of which preclude excessive use of IT resources for other than official purposes.

4. **DEFINITIONS:**

- a. **Staff Members.** Employees of the PBGC and employees of contractors assigned to projects, tasks, or any other related activities conducted for the benefit of PBGC under an active contract.
- b. **Official Business.** Any activity carried out by staff members in the performance of job assignments, duties, and responsibilities.
- c. **Office Equipment.** Equipment that includes, but is not limited to: laptop and desktop computers, peripheral equipment and software, telephones, copiers, handheld devices, facsimile machines, Internet connectivity and access to internet services and electronic mail.
- d. **Information Technology Resources.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information. Examples include desktop and laptop computers assigned to staff members.
- e. **Personal Use.** Personal use is any activity not to accomplish official PBGC business.
- f. **Unauthorized Software.** Computer applications not licensed, tested, and installed by PBGC, including shareware and freeware (for example, applications downloaded from the Internet).
- g. **Unauthorized Files.** Files that have no official business or purpose on PBGC's computers and include, but are not limited to files and software for which staff members do not have authority to use, because (a) materials for which staff members do not have copyrighted permission, (b) material that is proprietary, trademarked, or subject to intellectual property rights (beyond fair use); or, (c) material covered by the Privacy Act. Subject to the limited personal-use policy described below, file extensions that can identify unauthorized files include, but are not limited to: .AU, .AVI, .CDA, .GIF, .JPE, .JPG, .M1V, .MP2, .MP2V, .MP3, .MPA, .MPE, .MPEG, .MPG, .MPV2, .NRA, .NRB, .NRE, .NRG, .NRH, .NRI, .NRM, .NRU, .NRV, .NRV, .PCD, .RM, .VOB, .WM, and .WMA. PBGC recognizes that files with these extensions can have official business uses. The listing of these file extensions is intended to assist employees in complying with the policy.

5. **POLICIES:**

- a. **Authorized Uses and General Limits.** Generally, staff members may use office equipment and IT resources for official business only. Staff members may make limited personal use of office equipment and IT resources as set forth herein.

To achieve the stated goals of the policy, it is necessary to impose limits on the amount of IT resources used by staff members. In general and for all staff members the following limits are imposed for the resource indicated:

Resource	Limit
Individual Electronic Mailbox	400 Mbytes maximum
Individual Network File Storage ("H" drive or future equivalent)	500 Mbytes maximum
Electronic Mail Sent or Received (from external addresses)	10 Mbytes per message sent or received (including attachments)
Local Desktop Computer Hard Drive	67% of the capacity of the drive

Periodically, staff members will be provided with information concerning the amount of storage being used for electronic mailboxes, network file storage, and local desktop computer hard drives. Should staff members find that they are approaching or have exceeded the above limits, they should contact the OIT Help Desk to arrange for assistance in reducing the amount of resources used.

Should a staff member have a business need to transmit or receive an electronic mail message in excess of the size limit, that person should contact the OIT Help Desk to use alternative transmission modes (e.g., file transfer protocol) or to seek a one-time exception.

Should a staff member receive an electronic mail message in excess of the size limit shown above, the message will be quarantined and the OIT Help Desk will inform the intended recipient that he or she has a message in excess of the policy limit. The intended recipient may then ask the OIT Help Desk to deliver the message.

- b. Limited Personal Use of Office Equipment and Information Technology Resources.** To create a more accommodating work environment, PBGC allows staff members limited personal use of office equipment and IT resources. This policy does not create a right to use office equipment or IT resources for personal use, nor does it permit operation of a private business on one's own or another's behalf. Rather, this policy grants staff members the privilege to use office equipment and IT resources for limited personal use under the following general conditions. When such use:
- (1) involves little or no additional expense to the Government
 - (2) is performed during the staff member's non-work time
 - (3) does not interfere with the orderly, efficient operation of PBGC
 - (4) does not violate the Standards of Conduct of the Executive Branch.
- c. Guidelines and Examples of Personal Use.** The following guidelines are provided to further help delineate and clarify the meaning and intent of limited personal use. The

guidelines are not exhaustive, but serve to help staff members determine the bounds of limited personal use in commonly occurring situations.

- (1) The personal use incurs little or no additional cost to PBGC (such as electricity, ink, small amounts of paper, and ordinary wear and tear).
- (2) The personal use of occasional, short duration local telephone or fax calls or in the event of an emergency, the personal use of a long-distance telephone call or fax.
- (3) Infrequent sending and receiving of personal electronic mail messages, but not the sending or receiving of personal electronic messages with attachments greater than 100 kilobytes in size.
- (4) Limited personal use of the Internet for viewing web sites.
- (5) The use of a staff member desktop computer to play music or view video files for which the staff member has a license and which are contained on compact disks or other computer-readable, removable original distribution media. Sound volume shall be controlled to not disrupt or interfere with the work activities of other staff members.
- (6) Storing a limited number of personal digital photographs on the desktop computer hard-drive (C: drive) not to exceed 100 Mbytes of total storage.
- (7) Any file downloaded from the Internet or received via electronic mail, outside the conduct of official business, should be removed from all storage media (including electronic mail boxes, the desktop hard drive, C: drive, and any network storage) on a weekly basis. Written instructions advising staff members of the methods available for transferring files to removable media is contained on PBGC's Intranet system.
- (8) Personal use of premium web sites, such as Lexis/Nexis and Westlaw, must be during non-work time and at your own cost, billed directly to you.

d. IT Authorization Procedures. PBGC has established a corporate objective of maintaining licensing compliance for all software within the organization. PBGC is also required, pursuant to OMB Directive M-04-26, to ensure the appropriate use of all agency IT resources. In the event that a staff member or supervisor believes that a particular software, hardware, files, or other information technology is needed to achieve PBGC business objectives, it is the responsibility of the staff member and supervisor to seek prior written authorization from the Chief Technology Officer (CTO), or his authorized designee, before installing or using any such information technology on any PBGC equipment. The procedures for seeking CTO approval of information technology are contained in the *IT Authorization Procedures* available on the PBGC Intranet.

- (1) **Unapproved Software.** In the event that an unapproved software is necessary to conduct official business and there is insufficient time (e.g., impinging deadlines or other emergency conditions) to obtain prior written authorization, such software may be installed and used, but only after telephone and/or electronic mail notification to the individual's supervisor and the OIT Help Desk. Such

software may thereafter be removed or quarantined by OIT, subject to its evaluation as meeting the approval guidelines.

e. General Prohibitions.

(1) Prohibitions Subject to Disciplinary Action. The following use of office equipment and IT resources are prohibited, any violations of which may subject the PBGC user to immediate disciplinary action:

- (a) Illegal, unethical, or inappropriate activities, including activities which could be offensive to other staff members or the public. Such activities include, but are not limited to: electronic mail forgery, hate speech, and materials that ridicule others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.
- (b) Knowingly conducting private business or commercial matters (e.g., dealings with customers or clients associated with any second job a staff member may have). Staff members are prohibited from using work time, office equipment, or IT resources to maintain or support a private business. For example, a staff member may not use office equipment or IT resources (even during non-work hours) to run a travel business or accounting service. This absolute prohibition on using office equipment or IT resources to support a personal private business also prohibits staff members from using office equipment or information technology resources to assist relatives, friend, or other persons in such activities. However, this does not prohibit limited personal use of office equipment or IT resources for a non-profit, volunteer, or pro bono activity, provided such use is done on the staff member's non-work time.
- (c) Use of office equipment or IT resources as a staging ground or platform to gain unauthorized access to other systems.
- (d) Vulgar or obscene activity, such as sending Electronic mail or visiting an Internet site that has graphically violent or prurient sexually explicit material. In addition, staff members shall not create, download, view, copy, store, or transmit prurient sexually explicit or prurient sexually oriented materials.
- (e) Engaging in or obtaining information to engage in gambling, illegal weapons possession, terrorism or other illegal or prohibited activities.
- (f) Intentionally or knowingly damaging, disrupting, or attempting to damage or disrupt PBGC's office equipment or IT resources. This includes intentionally or knowingly releasing a computer virus.

(2) Prohibitions Subject to Warning before Disciplinary Action. The following actions are generally prohibited and will, if taken, result in a warning and advice as to how to avoid taking them in the future. Failure to heed the warning and

follow the advice may result in disciplinary action.

- (a) Advocating, or soliciting funds for political, religious, charitable, philosophical, or commercial causes, except for approved purposes such as the annual U.S. Savings Bonds drive, the Combined Federal Campaign, and certain Thomson School events.
- (b) Modifying office equipment and IT resources, including, but not limited to, loading unauthorized software or unauthorized files as defined in this policy, making computer system configuration changes, or attaching any equipment or device to office equipment or IT resources unless a part of their official duties, except by authorized OIT staff members in performance of assigned duties.
- (c) Any personal use that could cause congestion, delay, or disruption of service to any IT resources. For example, staff members may not:
 - (i) send electronic greeting cards or announcements in excess of 50 Kbytes in size through electronic mail or other means
 - (ii) send video or sound files, other than for PBGC business, or
 - (iii) use push or peer-to-peer technology or other continuous data streams which can degrade the performance of the network (peer-to-peer technology includes Instant Messenger and similar products and participation in chat rooms)
 - (iv) negligently damage or disrupt PBGC's office equipment or IT resources. This includes negligently releasing a computer virus, sending a chain letter electronic mail, or other act that could harm a computer or network.
 - (v) attempt to copy, delete, modify or read another's electronic mail without permission.
 - (vi) exceed the storage limits set out above.

f. Messages to Large Groups. In addition to observing file size limits, staff members are required to obtain approval before sending electronic mail, announcements, files, or messages of a personal or unofficial nature to groups of recipients. The approval levels for the following groups of recipients are shown below:

Group	Approving Official (or designee)
20 or more users	Department Director
FMA Members	FMA President
Fitness Center Members	Fitness Center Manager
Recreation Assoc.	Recreation Assoc. President
PBGC Toastmasters	PBGC Toastmasters President

Birth and death announcements within the affected person's department require no approval, but are subject to a maximize size limit of 50 Kbytes.

- g. Proper Representation.** It is the responsibility of every staff member to ensure they are not giving the false impression that they are acting in an official capacity when they are using office equipment or IT resources for personal purposes. This could include posting materials to external newsgroups, bulletin boards or other public forums. If there is a possibility that such a personal use could be interpreted to represent PBGC, an adequate disclaimer must be given. Acceptable disclaimer: *The contents of this message are mine personally and do not reflect any position of the U.S. Government or the Pension Benefit Guaranty Corporation.*
- h. Security Reviews.** Employees should have no expectation of privacy in their use of IT resources. PBGC conducts announced and unannounced security inspections of PBGC's computer resources, including electronic mail messages and files showing web sites visited. By using office equipment and IT resources, employees consent to disclose the contents of any and all files or information currently maintained on or previously passed through PBGC equipment. If employees wish their private activities to remain private, then they should not engage in those activities using IT and other office equipment resources.
- i. Remote Access.** Use only PBGC-approved software and procedures to view or transmit data when working at home or on travel. The OIT Help Desk issues approved software programs and remote access tokens. <http://owa.pbgc.gov> and <http://atwork.pbgc.gov> offer approved access to your electronic mail, files, and applications from any suitable web browser.
- j. Electronic Records Management.** Routinely saving all electronic mail messages and attachments slows the mail server and poses unnecessary administrative burdens to PBGC. If an electronic mail message or attachment is an official Federal record, then save it as required by *PBGC Directives IM 05-1, Electronic Recordkeeping* and *IM 15-1, Records Management*, or the *Federal Records Act*. Delete non-record material when no longer needed, then complete the delete by emptying electronic wastebaskets, both on desktops and within electronic mail accounts.

6. RESPONSIBILITIES:

- a. It is the responsibility of all executives, department directors, supervisors and team leaders to support the policies outlined and emphasize to PBGC staff members the importance of these policies.
- b. For technical help users should contact the OIT help desk .