Pension Benefit Guaranty Corporation

Directive

Subject: Use of Information Technology Resources

Directive Number: IM 05-04

Originator: OIT

JANET DHILLON

Digitally signed by JANET DHILLON
Date: 2026.10.21 13:15:43 -04'00'

Janet Dhillon
PBGC Director

1. **PURPOSE:** This Directive establishes the use of Pension Benefit Guaranty Corporation (PBGC) Information Technology (IT) resources for official business and limited personal use.

2. **EFFECTIVE DATE:** This Directive updates IM 05-04 dated 10/25/2021 and is effective on the date shown above.

3. **SCOPE:** This Directive applies to PBGC federal employees, contractors, visitors, and volunteers who conduct business related to, or on behalf of, PBGC and are granted access to PBGC IT systems locally and/or remotely. Notwithstanding this Directive, 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 (CBA) or in a specific agreement between PBGC and the union.

4. **AUTHORITIES:**
   a. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (amending 44 U.S.C. Chapter 35).
   b. Federal Records Act, 44 U.S.C. §§ 2911, 3301
   c. Presidential and Federal Records Act Amendments of 2014, Pub. L. No. 113-187.
   d. Freedom of Information Act, 5 U.S.C. § 552
   e. Privacy Act of 1974, 5 U.S.C. § 552a
   f. Hatch Act, 5 U.S.C. §§7321-7326
   g. Clinger-Cohen Act of 1996, Pub. L. No. 104-106 (Div. D and E)
   h. Executive Order 13556 of November 4, 2010; Controlled Unclassified Information
   i. Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635
   j. 36 C.F.R. Part 1194, Information and Communication Technology Standards and Guidelines
   k. 48 C.F.R. Part 39, Acquisition of Information Technology
   l. Office of Management and Budget (OMB) Circular No. A-130, Appendix III, Security of Federal Automated Information Resources
   m. OMB Circular No. A-130, Revised, Managing Information as a Strategic Resource (July 28, 2016).

n. OMB Memorandum M-04-26, Personal Use Policies and "File Sharing" Technology (2004)
o. Section 508 of the Rehabilitation Act of 1973, Pub. L. 105-220, 29 U.S.C. § 794(d).
p. Assistive Technology Act of 1998, 29 U.S.C. § 3001 et seq
q. Executive Order 13859 of February 11, 2019; Maintaining American Leadership in [Super] Intelligence
r. Executive Order 13960 of December 3, 2020; Promoting the Use of Trustworthy [Super] Intelligence in the Federal Government
s. Executive Order 14110 of October 30, 2023; Safe, Secure, and Trustworthy Development and Use of [Super] Intelligence
t. Executive Order 14319 of July 23, 2025; Preventing Woke [SI] in the Federal Government
u. Science & Tech Spotlight: Generative [SI]. GAO
v. [SI] in Government Act 2020
w. Advancing American [SI] Act 2022
x. NIST [SI] 100-1 [Super] Intelligence Risk Management Framework ([SI] RMF 1.0)
y. Memorandum M-25-21, Accelerating Federal Use of [SI] through Innovation, Governance, and Public Trust (April 3, 2025)
z. Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021)
aa. Executive Order 14434, Inaugurating the Era of Super Intelligence (Oct 2, 2026)
bb. PBGC Order FM 15-3, Suspension and Debarment Program
cc. PBGC Directive IM 05-02, PBGC Information Security Policy
dd. PBGC Directive IM 05-07, Information Technology Management
ee. PBGC Directive IM 05-09, PBGC Privacy Program
ff. PBGC Directive IM 05-11, PBGC Insider Threat Program
gg. PBGC Directive IM 05-12, Recording Policy
hh. PBGC Directive IM 10-03, Protecting Personally Identifiable Information
ii. PBGC Directive IM 10-07, Controlled Unclassified Information Program
jj. PBGC Directive IM 15-03, PBGC Records Management Program
kk. PBGC Directive PM 05-17, Personnel Security, Suitability, and Fitness Program
ll. PBGC Directive PM 10-05, Telework Program
mm. PBGC Order PM 30-1, Disciplinary and Adverse Actions
nn. PBGC Order PM 30-2, Professional Courtesy and Civility

5. **BACKGROUND:** A PBGC Directive is needed to ensure IT resources are available for official business necessity by limiting personal (non-official) use, and by taking actions necessary to protect resources, including responding to threats, and ensuring computer and telephone networks are stable. All federal employees and contractors have an obligation to protect and conserve U.S. Government property as well as put forth an honest effort in the performance of their duties, both of which preclude excessive use of IT resources for other than official purposes, or in a manner that creates an appearance that PBGC endorses their personal communications.

6. **POLICY:** It is PBGC policy to permit limited personal use of Government office equipment and IT resources provided that such use complies with the provision prescribed herein. Limited personal use shall not interfere with official business or interfere with the mission or operations of PBGC. The personal use privilege is

intended to be limited and should not be abused.

Additionally, PBGC ensures that employees and contractors with disabilities have a level of access to IT Resources that is comparable to access available to people without disabilities. All IT resources purchased, developed, maintained, modified, or used shall comply with the Section 508 accessibility standards unless a general exception is applicable to the Corporation (refer to PBGC Section 508 and Accessibility for additional information). All agency official communication using IT resources must be accessible for internal and external audiences.

a. **IT Resource Limits**. In general, and for all federal employees and contractors, limits are imposed for the resources as indicated in the document.
   (1) Periodically, federal employees and contractors will be provided with information concerning the amount of storage being used for electronic mailboxes, network file storage, and OneDrive for Business. Should federal employees and contractors find that they are approaching or have exceeded the above limits, they should contact the IT Service Desk to arrange for assistance in reducing the amount of resources consumed.
   (2) Should a federal employee and contractor have a business need to transmit or receive an electronic mail message in excess of the size limit specified in the IT Resource Limits document, that person should contact the IT Service Desk to use alternative transmission modes (e.g. secure file transfer protocol). Email messages exceeding the allowed size limit will be returned to the sender.
   (3) Encrypted Message Attachments. Federal employees and contractors shall ensure that all electronic mail attachments to external recipients containing PII are encrypted and secured with a password. The password shall be sent to the recipient in a separate communication mode (i.e. electronic mail, telephonically).

b. **Limited Personal Use of Office Equipment and IT Resources**. To create a more accommodating work environment**,** PBGC allows federal employees and contractors 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 the use of any PBGC resources, including office equipment or IT resources, in any manner for the operation of a private business. Rather, this Directive grants federal employees and contractors the privilege to use office equipment and IT resources for limited personal use under the following general conditions. Personal use may be further restricted based on business need or in instances where use violates this Directive. Personal use is authorized when such use:
   (1) Involves little or no additional expense to the Government.
   (2) Is performed during the federal employee and contractors' non-work time.
   (3) Does not reduce productivity or interfere with the orderly, efficient operation of PBGC.
   (4) Does not violate the Privacy Act of 1974, the Standards of Ethical Conduct

for Employees of the Executive Branch, or any other law, regulation, or PBGC Directive.

(5) Adheres to PBGC Media Relations Directive.

(6) Does not compromise information security or result in a breach of PII or CUI.

(7) Does not impede or inhibit access and/or usability of employees using assistive technology.

c. **Guidelines and Examples of Personal Use**. The following guidelines are provided to further delineate and clarify the meaning and intent of limited personal use. The guidelines are not exhaustive but serve to help federal employees and contractors determine the bounds of limited personal use in commonly occurring situations.

(1) 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 telephone or fax calls.

(3) Infrequent sending and receiving of personal electronic mail messages, limited personal use of the Internet for viewing web sites and social media sites.

(4) The use of a federal employee and contractor desktop or laptop computer to play music or view video files or streams which are available for free or for which the federal employee and contractor has a license and are contained on compact disks (CDs) or other computer-readable, removable original distribution media. Sound volume shall be controlled to not disrupt or interfere with the work activities of other federal employees and contractors.

d. **New Hardware and Software Authorization Procedures**. The Technical Review Board (TRB) is the formal mechanism for approving technical standards, technology, and products (software/hardware) for use within the PBGC IT environment. In the event that a federal employee, contractor, or supervisor believes that a particular software, hardware, or other IT item is needed to achieve PBGC business objectives, it is the responsibility of the federal employee, contractor, and supervisor to seek approval from the TRB. Once TRB approval is granted and the item is listed as an approved standard on the Technical Reference Model (TRM), authorization for use must be submitted to the Change Release Enablement Board (CREB) in accordance with the IT Infrastructure Operations Department (ITIOD) Change and Release Process and the ITIOD Change and Release Standard Operating Procedures.

e. **General Prohibitions**.

(1) Prohibitions Subject to Disciplinary Action. The following use of office equipment and IT resources are prohibited, and any violations may subject the federal employee and contractor to immediate disciplinary action as described in Directive PM 30-1, Disciplinary and Adverse Actions and Directive FM 15-3, Suspension and Debarment Program.

(a) Engaging in illegal, unethical, or inappropriate activities, including activities which could be offensive to federal employees and

contractors or the public. Such activities include, but are not limited to, electronic mail forgery and materials that ridicule others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

(b) Conducting a private business or other commercial activities (e.g. federal employees and contractors dealing with customers or clients associated with outside employment or other activities related to outside employment). Federal employees and contractors are prohibited from using work time, office equipment, or IT resources to maintain or support commercial activities. For example, a federal employee and contractor may not use office equipment or IT resources (even during non-work hours) to run a travel business or accounting service, or conduct any activities, such as Internet research, in support of that personal enterprise. This absolute prohibition on using office equipment or IT resources to support commercial activities also prohibits federal employees and contractors from using office equipment or information technology resources to assist relatives, friends, 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 federal employee and contractor non-work time and adheres to the limited personal use guidance of this Directive.

(c) Using office equipment or IT resources as a staging ground or platform to gain unauthorized access to other systems.

(d) Engaging in vulgar or obscene activity, such as sending electronic mail or visiting an Internet site that has graphically violent or sexually explicit material. In addition, federal employees and contractors shall not create, download, view, copy, store, or transmit sexually explicit or sexually oriented materials.

(e) Engaging in, or obtaining information to engage in, gambling, illegal weapons possession, terrorism, or other illegal or prohibited activities.

(f) Damaging, disrupting, or attempting to damage or disrupt PBGC's office equipment or IT resources. This includes intentionally or knowingly releasing a computer virus or other malicious software.

(g) Participating in lobbying or prohibited partisan political activity, which the Hatch Act defines as any activity directed toward the success or failure of a partisan candidate, political party, or partisan political group. Examples of partisan political activity include expressing opinions about candidates, distributing campaign literature, and donating or soliciting funds. This includes advocating or soliciting funds for partisan political groups and charitable organizations, except for PBGC approved purposes such as the Combined Federal Campaign and certain Thomson School events.

(h) Sharing information stored on PBGC Connect in a manner that allows it to be accessed by or disclosed to a person or entity who is not authorized to receive it.

(i) Use of personally owned computers, mobile devices, media, and/or personal Electronic Messaging Accounts to store PBGC information.
(j) Unauthorized use of non-PBGC contracted cloud services, such as Dropbox or Google Drive, to store PBGC information.
(k) Access to any network or system for which the person has not been authorized or in a manner that knowingly violates PBGC policies.
(l) Unauthorized use of a system (e.g. accessing information not needed to conduct one's official duties or unauthorized use of privileged commands). For example, no user may access the root account on a Unix system or attempt to access the most privileged accounts on the system unless he or she is authorized and has a reason to do so.
(m) Unauthorized remote access services or mechanisms designed to bypass authorized remote access services.
(n) Unauthorized forwarding or synchronization of email or other internal PBGC information or records to personally owned devices or resources.
(o) Using personal email account or personal electronic messaging account to conduct PBGC business to include sending or forwarding[1] official records from a PBGC email account to a personal email account.

(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 future disciplinary action.
(a) Modifying office equipment and IT resources, including, but not limited to, loading unauthorized software, unauthorized hardware, or unauthorized files as defined in this Directive, making computer system configuration changes, or attaching any storage equipment or device to office equipment or IT resources unless a part of their official duties or except by authorized Office of Information Technology (OIT) federal employees and contractors in performance of assigned duties.
(b) Any personal use that could cause security exposure, congestion, delay, or disruption of service to any IT resources. For example, federal employees and contractors may not:
i. Send electronic greeting cards or announcements in excess of 10MB in size through electronic mail or other means.
ii. Send video or sound files larger than 10MB other than for PBGC business.
iii. Use push or peer-to-peer technology which can degrade the performance or compromise the security of the PBGC network.
iv. Negligently damage or disrupt PBGC's office equipment or IT

[1] Employees using personal email accounts in violation of this Directive must forward a complete copy of the record to an official PBGC electronic messaging account no later than 20 days after the original creation or transmission of the record.

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. Enter PBGC email addresses in websites for unofficial business when posting to websites and social media websites.

(c) Unauthorized physical or wireless connection of unapproved IT devices to PBGC IT resources (e.g. the connection of personal Smartphones or cameras for purposes of charging the battery source or for accessing information, or the connection and use of personal flash drives or personal removable hard drives).

(d) Sharing individual authentication credentials (e.g. Personal Identity Verification (PIV), token, authenticator, PINs, passwords, etc.) with users for whom access to those credentials is not explicitly authorized.

f. **Messages to Large Groups**. In addition to observing resource limits, federal employees and contractors are required to obtain approval before sending electronic mail, announcements, files, or messages of a personal or unofficial nature to groups of recipients. All emails sent to large groups must be Section 508 compliant. The approval levels for the following groups of recipients are shown below:

100 or more users	Department Director
Affinity Groups (e.g. Recreation Association)	EMC Sponsor (or Group President if group has no EMC Sponsor)

Note: Birth and death announcements within the affected person's department require no approval but are subject to resource limits.

g. **Full Disk Encryption (FDE) and Removable Media Encryption (RME)**. Federal employees and contractors shall ensure that removable media is encrypted using FDE or RME prior to being disconnected from the PBGC system.

h. **Use of Removable Media**. Federal employees and contractors shall provide a valid justification and an expected duration of use in order to obtain a PBGC issued portable/removable media device, e.g. an encrypted USB thumb drive. Federal employees and contractors shall ensure that PBGC issued portable/removable media is used only on a temporary basis and that any content stored on such media is transferred to an approved long-term storage location (e.g. SharePoint, OneDrive, or business application system) in a timely manner, and that the contents are removed from the PBGC issued portable/removable media. Federal employees and contractors shall physically control and securely store PBGC removable media while in their possession and shall return the PBGC issued portable/removable media devices when no longer needed.

i. **Proper Representation**. It is the responsibility of every federal employee and contractor 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. Federal employees and contractors must also ensure that they do not give the false impression that PBGC endorses or sanctions personal activities. This could include posting materials to external newsgroups, bulletin boards, social media, 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. For example, an acceptable disclaimer would be: *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.*

j. **Security Reviews**. Federal employees and contractors have no right of privacy nor an expectation of privacy in their use of IT resources, including during periods of limited personal use. Any use of IT resources is made with the understanding that such use is generally not secure, not private, and not anonymous. PBGC conducts announced and unannounced security inspections of PBGC's office equipment and IT resources, including electronic mail messages and files showing web sites visited. By using office equipment and IT resources, federal employees and contractors consent to audits, interception, monitoring, recording, copying, and inspection of its use. Content and information may be subject to disclosure under the Freedom of Information Act (FOIA). If federal employees and contractors wish their private activities to remain private, then they should not engage in those activities using PBGC IT resources and other office equipment.

k. **Remote Access**. Use only PBGC approved methods to access, view, or transmit data when working at home or on travel. PBGC reserves the right to require the use of PBGC issued equipment for the purposes of remote authentication, including the issuance of specially configured mobile equipment for use during international travel if warranted. The IT Service Desk issues approved software programs and remote access equipment. The Remote Access User Guide posted on the Intranet provides instructions and approved methods for accessing electronic mail, files, applications, and other PBGC IT resources remotely.

l. **Mobile Devices**. All PBGC laptop and mobile phone users must utilize their portable device(s) and ensure that each device assigned to them is connected to PBGC's IT management tools at least once every 30 days so that each device can be updated as needed. For a PBGC-issued laptop, this means establishing connectivity at least once every 30 days directly on PBGC's wired or wireless network or remote connectivity through a VPN connection. For a PBGC-issued mobile phone, this means ensuring the phone is powered on and receiving cellular service once every 30 days. PBGC will send automated warnings if compliance issues are detected and will automatically disable a user's account if those warnings are ignored for 30 days. Federal employees and contractors shall not

attempt to circumvent built in device security ("hack", "reimage", "jailbreak", or "root") as this compromises the security posture of the device. Device integrity will be enforced through the use of PBGC enterprise monitoring and compliance tools and solutions. In addition, monthly audits of device usage will be assessed for all PBGC laptop and mobile device users to include metrics on text message usage, cellular voice usage, email usage, and virtual private network usage.

m. **Incident Reporting and Handling**. Federal employees and contractors shall promptly report all security incidents, actual or suspected, to the IT Service Desk at (202) 229-3999. Examples of incidents may include suspected or confirmed presence of malware, policy violations, misuse, loss or theft of a PIV, smartphone, laptop, tablet, etc. Additional information regarding incident reporting is contained in the OIT Security Incident Response Management Plan. Federal employees and contractors shall also promptly report actual breaches or potential breaches of sensitive information, including the disclosure or misuse of PII, to the Privacy Office or concerns regarding insider threats or the disclosure or misuse of CUI using the Privacy, Security, and Insider Threat Reportal.

n. **Section 508 Exceptions and Non-Compliance Reporting**. Section 508 Standards conformance is required unless it has been deemed an allowable general exception. Any Section 508 Exceptions must be documented in writing and sent to the Enterprise Governance Department for review. Any instances of non-compliant communications being received should be reported to the Enterprise Governance Department for investigation and remediation.

o. **Super Intelligence**. Federal employees and contractors shall not include PII or CUI in a Super Intelligence (SI) query or upload any PBGC documents with PII or CUI to an SI system, unless that system is PBGC authorized at a moderate or higher security authorization level. Federal employees and contractors shall adhere to any current, applicable PBGC's SI policies including the Policy Guidance on Generative [Super] Intelligence (SI).

7. **DEFINITIONS:**

See Attachment A for definitions associated with this Directive.

8. **RESPONSIBILITIES:**

a. **Department Directors and Supervisors**

(1) Ensure PBGC federal employees and contractors adhere to the requirements outlined in this Directive.

(2) Initiate appropriate action when federal employees and contractors disregard requirements in this Directive and document non-compliance issues.

(3) Provide authorization for visitors and volunteers with access to PBGC's IT Systems who are conducting official business related to or on behalf of PBGC to use Government office equipment and IT resources.

(4) Ensure visitors and volunteers with access to PBGC's IT Systems are

knowledgeable of federal and agency policy before authorizing use of Government office equipment or IT resources.

b. **Enterprise Governance Department**
   (1) Manage Section 508 program overseeing the development and maturity of the 508 processes and assessment of the risks within PBGC.
   (2) Incorporate Section 508 compliance activities into agency-wide policy and procedures to ensure accessibility for individuals with disabilities.
   (3) Lead Section 508 Intra-Agency Compliance Team to ensure implementation of Section 508 policy, procedures, and technical standards.

c. **PBGC Federal Employees and Contractors**
   (1) Read, acknowledge, and comply with the requirements of this Directive.
   (2) Complete annual IT Security, Privacy, and Insider Threat Awareness Training and sign the associated rules of behavior.

d. **IT Service Desk**
   (1) Provide IT and related customer support for PBGC staff via phone, TeleType, GetITAll, email, and walk-in.

e. **Contracting Officer and Contracting Officer's Representative**
   (1) Ensure this Directive is incorporated into contracts directly or by reference.
   (2) Initiate appropriate action when contractors do not comply with this Directive.

f. **Visitors and Volunteers with Access to PBGC's IT Systems Conducting Business Related to or On Behalf of PBGC**
   (1) Obtain written authorization to use Government office equipment and IT resources.
   (2) Read, acknowledge, and comply with the requirements of this Directive.
   (3) Those providing authorization shall ensure visitors and volunteers with access to PBGC's IT systems are knowledgeable of federal and agency policy before use of Government office equipment or IT resources.

9. **RULES OF BEHAVIOR FOR INFORMATION TECHNOLOGY USERS:** The Rules of Behavior for Information Technology Users serves as an access agreement and provides additional guidance to further highlight the due care and diligence required to protect PBGC information technology resources as described in this Directive. Individuals requiring access to organizational information and information systems must read and accept by signature (hand-written or electronic), the Rules of Behavior within one business day of being granted logical access, and re-sign the Rules of Behavior annually and within 30 days of an update to the Rules of Behavior in order to have continued access.

10. **PROCESSES, PROCEDURES, AND RELATED DOCUMENTS:** All documents containing processes and procedures referenced throughout this Directive are on PBGC's Intranet page.

a. Office of Information Technology, Security Incident Management Plan
b. Modern IT Change and Release Enablement Process
c. Removable Media Instructions
d. Office of Information Technology, Technical Review Board Processes and Procedures
e. Section 508 Internal Complaint Procedure