PBGC Information Security Policy

1. Purpose.

The Pension Benefit Guaranty Corporation (PBGC) Information Security Policy (ISP) defines the security and protection of PBGC information resources.

2. Reference.

Office of Management and Budget (OMB) Circular A-130, The Computer Security Act (Public Law 100-235), Executive Order 13103 and other applicable guidelines and laws.

3. Applicability.

The provisions of the ISP apply to all Pension Benefit Guaranty Corporation (PBGC) employees and contractors (hereby known as PBGC staff) who use and access a portable computer or computer system to process information for the PBGC.

4. Interim Policy.

It is the policy of the PBGC to apply the maximum cost-effective level of protection to PBGC Information Systems (IS), and to comply with applicable Federal statutes, regulations, policies, standards and guidelines.

5. Responsibilities.

a. PBGC Executive Director shall:

Designate a senior official to have the primary responsibility for developing, monitoring and disseminating PBGC's ISP.

b. Chief Information Officer shall:

Establishes the PBGC's computer security program and is responsible for overseeing the program goals, objectives, and priorities in order to support the mission of PBGC.

c. Director, Information Resources Management Department (IRMD) shall:

(1) oversee the development, maintenance and dissemination of the PBGC's ISP;

(2) appoint an Information Systems Security Officer (ISSO); and

(3) review and approve information security policies, standards, procedures, architecture and implementation plans developed by the ISSO.

d. Information Systems Security Officer (ISSO).
The ISSO shall:

(1) develop, maintain, implement and manage the ISP and act as the PBGC IS security focal point;

(2) develop PBGC IS security strategy, standards, and architecture;

(3) ensure in coordination with the PBGC Training Institute that IS security staff, PBGC managers, users, system administrators, contractors are provided effective security awareness training in compliance with the PBGC Computer Security Awareness and Training Program guidelines;

(4) coordinate IS security plans, risk analyses, contingency plans and certifications with FASD, department representatives and IRMD staff;

(5) assist the PBGC Disclosure Officer in the location and review of computerized record systems;

(6) develop the capability to conduct periodic announced and unannounced security inspections, and/or reviews of computer files of PBGC IS users in accordance with the PBGC Audit and Monitoring Policy;

(7) document and advise the PBGC Inspector General on matters pertaining to the illegal or unauthorized use of PBGC computer resources;

(8) coordinate security procedure functions with the PBGC Inspector General;

(9) establish a management control process to ensure that appropriate administrative, physical, and technical safeguards are incorporated into existing and new IS applications and information technology infrastructure;

(10) respond to IS security incidents in a timely manner, report to management on a regular scheduled basis on security incidents and maintain documentation of any suspected security violation;

(11) develop, in coordination with the PBGC Procurement Department and the originating department, computer security requirements and appropriate contractual clauses for solicitations and contracts for the acquisition or operation of computer facilities, equipment, software packages and/or related services;

(12) certify that contractor operated PBGC IS meet documented and approved security specifications/standards and comply with applicable Federal regulations, policies and standards prior to and after implementation; and

(13) establish procedures to ensure that PBGC customer's rights to privacy, as stated in the Privacy Act of 1974 and the Freedom of Information Act (FOIA), are protected and that the integrity of data is maintained.

e. <u>IRMD, Help Desk</u>.
The IRMD Help Desk shall:

(1) support PBGC staff with problems related to the security of hardware and software systems. This support includes the technical assistance, software procedures, and instruction necessary to clean up virus infected PCs and diskettes;

(2) issue and reset user ID passwords on PBGC IS;

(3) document and immediately notify the ISSO and the LAN Administrators whenever a breach of PC or LAN security becomes known in accordance with the <u>PBGC Computer Security Incident Procedures</u>; and

(4) provide direct user support for questions dealing with systems hardware/software and user access in accordance with the <u>IRMD Help Desk/LAN Administrators Standard Operating Procedures Handbook.</u>

f. <u>Department Directors</u> shall:
(1) report any known or suspected misuse of computer resources to the ISSO;

(2) select a department representative to coordinate security-related efforts with the ISSO, as requested;

(3) control access to computer-related equipment located in their department to ensure that resources are used for PBGC business activities; that computer resources are only used by authorized personnel; that equipment is secured from theft and unauthorized use;

(2) identify sensitive systems, applications, and files which are department controlled and request the assistance of the ISSO to identify sensitive information resources in accordance with the PBGC Access and Physical Security Procedures; and

(3) provide written authorization for approving users access to information resources.

g. The Inspector General shall:

(1) conduct reviews of data in computer files of individual users when an on-going investigation indicates that there is probable cause to believe that a violation of law, regulation or the policies is occurring; and

(2) perform evaluations of the security controls for the information technology management that PBGC data, applications, and systems are adequately protected against risks which could result from the inadvertent or deliberate disclosure, alteration, or destruction.

h. PBGC Disclosure Officer shall:

(1) coordinate with Department Directors and/or their representative(s) to determine the sensitivity of data on PBGC's IS;

(2) coordinate with the ISSO to ensure that the record safeguards mandated by the Privacy Act of 1974 are maintained on all PBGC IS;

(3) determine if data maintained in PBGC IS can be disclosed based on PBGC disclosure guidelines; and

(4) ensure that systems of records maintained in computerized format are included in PBGC's System of Records announcements in the Federal Register as required by the Privacy Act of 1974.

i. **The Human Resources Department.**
PBGC Security Officer will arrange for suitability determinations of PBGC staff in IS related positions in accordance with Federal laws, regulations and Executive Orders.

j. **The PBGC Contracting Officer shall:**

(1) **assure that the ISSO is consulted during the planning phase of all IS related solicitations;**

(2) **be responsible for ensuring that all IS-related solicitations and contracts contain provisions for computer mandated security requirements;**

(3) **ensure that contractors of PBGC projects are aware of their responsibility to assign only contractor staff who can meet certain suitability criteria.**

(4) **include the responsibilities assigned by the PBGC ISP to PBGC Contractors in the appropriate contractual document(s); and**

(5) **verify that PBGC contract staff are following the guidelines in the PBGC Separation Clearance Procedures for Contract Staff.**

k. **Local Area Network (LAN) Administrator.**
Each LAN Administrator shall coordinate IS Security procedures with the ISSO and follow guidelines as outlined in the IRMD Help Desk/LAN Administrators Standard Operating Procedures Handbook. The LAN Administrators shall implement security controls within network elements and servers in accordance with PBGC platform security standards.

l. **Authorized PBGC IS Users.**
Security of information cannot be the sole responsibility of the ISSO and Department Directors. The PBGC IS user determines the effectiveness of most security safeguards. PBGC staff who work with PBGC IS resources shall:

(1) **immediately report known or suspected unauthorized use or disclosure of user ID's and/or passwords, misuse of computer resources, violations of security, or unusual occurrences to the IRMD Help Desk and his or her immediate manager;**

(2) notify the Inspector General of any known or suspected thefts, and other known or suspected criminal activity related to PBGC IS resources;

(3) be aware of, and understand their responsibility to comply with the ISP;

(4) use PBGC IS resources only for lawful and authorized PBGC business purposes as defined in the PBGC Electronic Communications Policy;

(5) recognize his/her accountability for all activity taking place with his/her personal user ID in accordance with the PBGC Password Usage Policy ;

(6) comply with any safeguards, policies, or procedures that prevent accidental or deliberate access by unauthorized persons to IS resources and/or sensitive information;

(7) comply with safeguards and procedures that prevent unauthorized access to PBGC IS via a modem as outlined in PBGC Modem Usage Policy;

(8) comply with the terms and conditions of licensed software that is authorized for use at PBGC in accordance with the PBGC Software Management Policy;

(9) not copy licensed PBGC software as outlined in the PBGC Software Acquisition Policy;

(10) attend Computer Security Awareness Training as outlined in the PBGC Computer Security Awareness and Training Program guidelines; and

(11) understand that PBGC reserves the right to confiscate and remove unauthorized software and hardware and to take disciplinary action against those PBGC employees who do not comply with the PBGC ISP.

m. Contracting Officer's Technical Representative (COTR) shall:

(1) Ensure the contractor designates a security representative who will:

(a) coordinate all IS security procedures with the ISSO;

(b) ensure that all contractor personnel are informed of, and comply with, PBGC security related policies, procedures and directives;

(c) ensure compliance with any written security related instructions from the ISSO; and

(d) promptly report known or suspected unauthorized use, or disclosure of user ID's and/or passwords, misuse of computer resources, violations of security, or unusual occurrences to the IRMD Help Desk and his or her immediate manager; and

(e) initiate the PBGC Form 169C "Separation Clearance for Contract Staff" for each departing contract employee in accordance with the PBGC Separation Clearance Procedures for Contract Staff.

NOTE: PBGC Contract Staff at FBA sites, will have the PBGC Form 169C initiated at the site and forwarded to their COTR or designee for completion and routing to the IRMD Help Desk in accordance with the PBGC IOD WAN Manual, Section 4.1 "New WAN Account Requests and Employee Separation Procedures."

(2) Provide a list of on-site/off-site personnel working on contracts who require IS privileges, including job title and function to the ISSO.

n. Facilities and Services Department.
Shall arrange for suitability determinations of contractor personnel in IS related positions.

6. Obtaining Access to PBGC IS.
IRMD has established procedures which, in conjunction with appropriate request forms, will allow personnel to access PBGC IS. These forms are available from the IRMD Help Desk and must be properly completed by PBGC staff and submitted to the IRMD Help Desk to obtain access in accordance with the PBGC Access and Physical Security Procedures.

7. Employee or Contractor Departing PBGC.
PBGC staff who have access to PBGC IS, must have all access to PBGC's IS terminated before departing the Agency. PBGC Federal employees and contract staff must obtain or initiate either PBGC Form 169 "Separation Clearance for Federal Employees" or PBGC Form 169C "Separation Clearance for Contract Staff" in accordance with the guidelines stated in the "Separation Clearance

Procedures for Federal Employees or Contract Staff".

The ISSO and responsible LAN Administrator must ensure that systems access is terminated and files are transferred to the individual manager for retention

determinations in compliance with the IRMD Help Desk/LAN Administrators Standard Operating Procedures Handbook.

8. Emergency Systems Access Termination.
PBGC managers, COTRs, or contractor managers who wish to have computer access authorization revoked or terminated for PBGC staff in an emergency should immediately contact the IRMD Help Desk. The IRMD/CSD Manager will ensure that proper measures are invoked to protect information and computer resources accessible through the User ID. The requestor of an emergency termination action must follow-up with the appropriate PBGC request form(s) as outlined in the IRMD Help Desk/LAN Administrators Standard Operating Procedures Handbook.

9. Access Control for PBGC's Data Center.
Access to IRMD Data Center is controlled at all times. Authorization for gaining access to the Data Center will be granted solely by the IRMD Data Center Facilities Management COTR or the Manager, IRMD/Technical Infrastructure Division. Authorized visitors can gain escorted access to the Data Center via the IRMD Help Desk. Visitors must obtain approval from the supervisor of the Data Center when requesting access during other than normal working hours.

10. Ownership and Management Responsibility.
Ownership of PBGC IS, resources, and equipment resides with the department purchasing the peripheral(s), managing the data or developing the applications. Department Directors should assign ownership to a PBGC organizational entity. Owners' responsibilities should not be construed as replacing or diluting the ISSO's or the Department Directors' responsibilities for compliance with IS security requirements.

The designated owners of PBGC's various IS assets have the responsibility to:

a. acknowledge ownership of resources and identify those containing or processing sensitive data as defined in the PBGC IS Containing Sensitive Data Guidelines to the ISSO;

b. coordinate with the ISSO to develop protection controls;

c. authorize access to resources under their control;

d. educate managers and users on control and protection requirements as established in the PBGC Password Usage Policy and the PBGC Modem Usage Policy.

e. monitor compliance with established security regulations, directives, and circulars and periodically review control processes; and

f. participate in risk assessment and developing contingency plans, when necessary.

11. Disaster Recovery and System Availability.
Ownership of the PBGC IS COOP is under the IRMD/Technical Infrastructure Division. These plans are developed and implemented to facilitate the timely restoration of PBGC computer, network, telecommunications equipment and business processing applications and underlying infrastructure in the event of an unscheduled disruption.

12. PBGC IS Change Management.
PBGC staff responsible for system hardware and software changes, must adhere to the procedures described in the PBGC Change Management Handbook for initiating and completing changes to the PBGC IS network(s). These procedures include submitting change requests, notification procedures, participation in change meetings, coordinating activities, approval processes, testing of new applications, installing test servers, and actual implementation of changes.