

PBGC Access and Physical Security Procedures

Introduction

Access to the physical security of all PBGC facilities nation-wide is coordinated by the Facilities and Services Department (FASD). FASD and IRMD staff maintain a working relationship to ensure the safety and security of PBGC Information Systems (IS). PBGC personnel (employees and contractors) have a responsibility to ensure that only authorized staff have access to these facilities.

1. Access Controls

PBGC personnel have a responsibility to create and maintain a secure work environment, and to protect the computer assets used to fulfill PBGC business activities. Access to offices and work areas, where PBGC information, PCs, and LAN resources are located, should be controlled in a manner that permits access only to authorized persons.

The controls needed in PBGC business areas depend upon the information resources housed in the area and the level of exposure. PBGC management and System Administrators should implement the following controls to protect information assets under their control:

- (a) Ensure that PBGC personnel have only one (1) general USER ID account to access PBGC Information Systems (i.e., electronic mail, INTERNET, word processor, etc) for daily PBGC business activities.**
- (b) Ensure that LAN Administrators, developers, testers, etc., only access PBGC IS with their unique USER ID account to perform administrative LAN/System maintenance and support.**
- (c) Ensure that PBGC personnel understand their responsibility for maintaining a secure and safe work area and that each individual take reasonable measures to assure the security and safekeeping of the PC and LAN information resources being used.**
- (d) Ensure that access to areas housing IS are securely controlled and that persons authorized to access a secured area are PBGC personnel, or if a visitor that they are accompanied by PBGC personnel.**
- (e) PBGC does not permit guest USER ID accounts on it's IS and all USER ID accounts must have a unique password created in accordance with the PBGC Password Guidelines and Procedures.**

2. Preventing Hardware Theft

Information and computer equipment must be protected against theft. Loss of certain information, if not properly backed-up, can require significant effort to recreate it. Serious repercussions will ensue if the lost information is subject to Privacy Act or FOIA compliance. It is the responsibility of PBGC Department Directors to determine the likelihood of theft of resources in their control and implement the controls to limit or nullify an exposure to theft.

Department Directors should implement the following anti-theft controls, as appropriate.

- (a) Only authorized PBGC personnel should have access to areas where computer resources are housed. Authorization to controlled areas should be granted, and removed when applicable, on a "need to access basis."**
- (b) Work areas, storage areas, and offices housing PBGC IS should have locked doors, cabinets, or desks, in use. When computer hardware is not secured, it should be secured with equipment enclosures and/or lock-down devices. Accessory equipment like modems and external disk drives should be secured in a similar fashion.**
- (c) Sensitive correspondence, reports and spreadsheets in hard copy form or on magnetic media must be stored in locked containers, desks or files.**
- (d) PBGC personnel should monitor computer resources during business hours if the resources are not in a lockable area.**
- (e) Departments utilizing a Projection System and a PC to connect to PBGC IS must adhere to the following:**
 - (1) Department Directors will establish key points of contact for access;**
 - (2) use a physical security device to keep the PC secure;**
 - (3) develop access request procedures to ensure proper startup and shutdown of the PC;**
 - (4) use a single login (auto-login) to limit the cross container and program distribution errors;**
 - (5) establish a virtual security (if needed) to ensure shutdown if the PC is left unattended;**
 - (6) ensure passwords for all PCs are identical. If problems occur they are resolved quickly;**

- (7) ensure user accounts are locked or hard coded by MAC address to a particular PC for access; and
- (8) the PC should never be left unattended while powered on.

NOTE: The above security guidelines do not take into effect the issues that are involved with installing pcAnywhere and establishing remote access to these PCs. If this is to be done, additional issues will become apparent. If PBGC establishes remote access to these PCs in the future, additional security consideration will need to be addressed.

3. Portable Computer Resources

Hardware and software techniques should be employed to keep PBGC information protected from unauthorized individuals in the event the portable PC equipment is lost or stolen. Options include, but are not limited to, lock-down devices and PC-boot passwords.

PBGC personnel should be particularly security conscious when traveling with portable computer resources. Measures must be taken to ensure that PBGC personnel are educated on security practices when traveling with portable resources. PBGC personnel having portable computer resources will be given information on the methods to safeguard the resource they are receiving.

4. Removable Information Media

Removable media, such as hard copy and diskettes, may contain large concentrations of sensitive data vital to the PBGC. When sensitive data is stored on removable media, necessary access controls should be employed by management to ensure the protection of sensitive PBGC information. Depending on the exposure and sensitivity of information residing on removable media, management should establish any or all of the following controls:

- (a) Ensure that PBGC personnel understand the significance of sensitive information contained on removable media. Additionally, advise PBGC personnel of their responsibility to protect information on removable media as protection of this information would be required in other formats;
- (b) Discard hard copy information in an authorized and secure manner that prohibits the information from being retrieved and made use of by unauthorized persons; and

- (c) **Develop procedures to ensure that sensitive information is not stored on diskettes unless the diskettes are properly labeled and stored in a lockable unit.**

5. Relocating Computer Hardware

PCs and related hardware are often moved from one location to another. It is important that secure methods are employed to safeguard this equipment and the information it may contain during relocation. PBGC personnel must contact the IRMD Help Desk to move any and all PBGC IS hardware by initiating a Technical Assistance Request (TAR). In special circumstances, requests for LAN Administrators to relocate hardware will be accepted, in advance, by the IRMD Help Desk and will be considered on a case-by-case basis.

PBGC personnel removing agency owned computer equipment from PBGC facilities to their home, another office, etc., are required to obtain a property pass from their authorized department property managers.

Requests to move equipment at FBA sites, will be coordinated through the PBGC WAN team.

6. Environmental Protection

PCs are sensitive to the quality of electrical power. Smoking, drinking, and eating should be discouraged in the immediate vicinity of PCs and other peripherals.

7. Network Systems Inventory

IRMD is responsible for maintaining an up-to-date register of PBGC and departmental computer assets. PBGC computer resources shall be assigned a unique configuration number by IRMD. All hardware shall be marked clearly with this number. LAN Administrators should coordinate with IRMD to ensure that hardware and software computer resource inventory reports are accurate and up to date. Any inventory report change or correction should also be coordinated with the IRMD Help Desk. As a general guide, the information gathered should include, but is not limited to:

a. Hardware

- (1) Equipment description;**

- (2) **PC peripherals;**
- (3) **Serial number;**
- (4) **Date installed;**
- (5) **Vendor/manufacturer name;**
- (6) **Physical equipment location;**
- (7) **Assigned equipment user; and**
- (8) **Internal PC cards and add-on components.**

b. Software.

- (1) **Original Purchase Order (P.O.) request;**
- (2) **Software description and documentation;**
- (3) **Software serial number;**
- (4) **Software version number;**
- (5) **Date installed;**
- (6) **Vendor/manufacturer name;**
- (7) **Number of copies purchased/leased;**
- (8) **A copy of the software registration card; and**
- (9) **A copy of all warranties included in the purchase.**