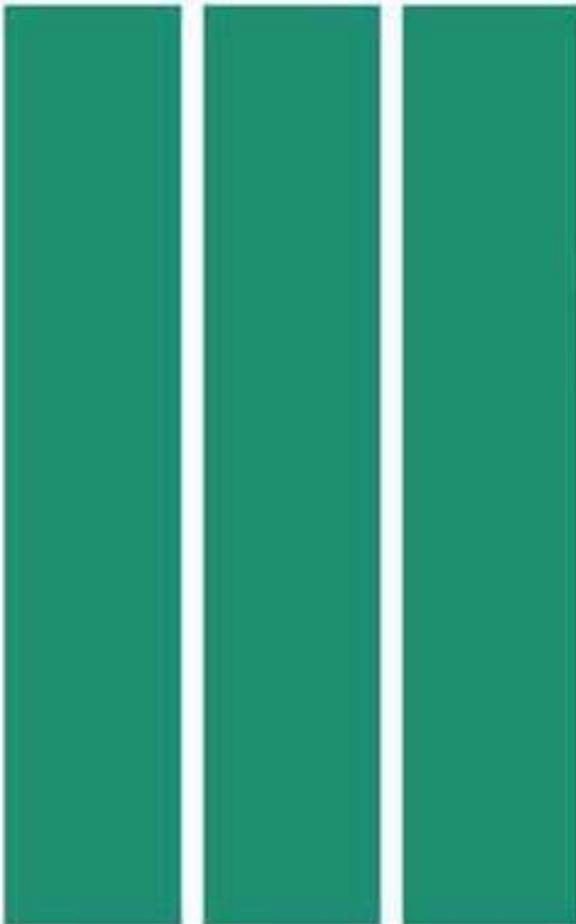




**PIC HELP NEWSBRIEF**

March 2003 Volume 2, Issue 3



# Special Edition on Security

## Introduction

Security is an important but unexciting topic. A poor security program can be disastrous for the business or agency. There are too many instances of PHAs losing all or part of their data due to a lax security program. This article is not intended to replace security training or to make you an “instant security expert.” It is intended to call your attention to some important aspects of security to help you avoid the disaster. You should still attend a formal training class in system security and disaster recovery. They are available at most community and junior colleges.

Data has value. If it takes four hours for someone paid \$12.50 per hour to create a report, then the direct cost of that report is \$50 (disregarding the associated costs). It would cost \$50 to recreate it if it were lost. Many types of business data have much greater intrinsic value because of the way the data is used, where it comes from or the purpose it fulfills.

Data can be deleted, damaged, distorted, or disclosed to people with no business having access to the information. Disgruntled ex-employees, hackers, unethical business competitors, and identity thieves all have motives for unauthorized access to data.

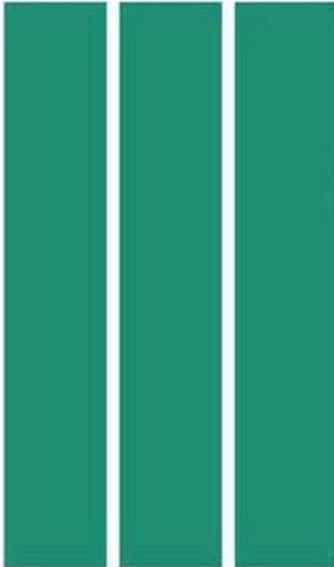
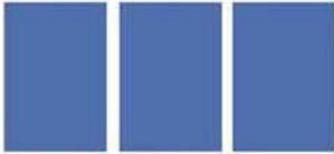
In addition, we in public service, have the Privacy Act to follow. We must protect the privacy and accuracy of the personal data about people that we compile and handle in doing our jobs. Data about tenant families; rent payments, agency staff, business contacts, and staff payrolls all falls under the Privacy Act.

### Security Issues.

- Physical and system security – Keeping people away from access to the data.
- Data backups – Making copies of data in case of data damage or destruction.
- User access security – controlling access to data and authenticating user identity.
- Security plans and procedures – the established ways of carrying out security responsibilities.

## **INSIDE THIS ISSUE**

<b>2</b>	Introduction
<b>3</b>	Physical & system Security
<b>3</b>	Data backups
<b>4</b>	User Access security
<b>5</b>	Security plans & procedures
<b>6-7</b>	Good Security Practices
<b>8</b>	Announcements



## **Physical and system security**

Office workers frequently log into a system then leave the desk to run an errand without logging out. A visitor to the desk could gain unauthorized access to the system. Sometimes LAN servers are installed in a room that is not kept securely locked. An intruder could delete or damage the database files on the server. Backup copies of data files or paper printouts may be stored on a bookshelf in the office from where they can be carried away and viewed.

Controlling physical access to staff members' desks, the computer room, and data physical storage areas is required for an effective security program. User IDs and passwords and confidential information printed on paper must also be protected.

## **Data backups**

Everyone knows data backups are important but they are the first thing overlooked when things get busy. Why? Data backups are time consuming and boring, like buying fire insurance. But they are (like fire insurance) vital as a strategy for ensuring survival of the agency's operations in case of disaster.

There are many methods and technologies for making data backups. We won't cover them here. Key principles involve making the backup copy on a regular schedule using a separate medium and keeping copies stored securely away from the location of the original data. Otherwise, the backups can be lost or destroyed at the same time that the original data is lost or destroyed. Backups should be kept in a separate building or transmitted to an off-site backup storage service to ensure survivability. The time interval between backups should be based on the amount of work you can afford to lose.

In addition, the quality of the backups should be tested periodically. Woe to the agency that loses its data because of a server disk crash then finds out that the backup copy is blank or corrupted.



## User access security

User access security consists of a combination of procedures and system configurations that limit an authorized user to access only the data necessary to carry out his or her duties and responsibilities. This is done by (1) segregating and controlling individual access to different parts of the data systems, (2) the use of user identification, and (3) user authentication.

- ***Segregating individual access to data systems*** – Not all staff members need full “edit” access to all data. Some may only need read-only access or no access at all. This is a management judgment to balance the office efficiency and security needs with minimum risk. For example, a receptionist needs to know the names and phone numbers of staff members and tenants but not the tenant payment amount or the staff pay grade. Maintenance staff only needs access to tenant names, addresses and phone numbers and maintenance records.

Management must maintain records concerning who has been granted access to what parts of data systems, what type of access is granted to them, and who authorized the access. These access rights should be reviewed annually for relevance and access need.

- ***User identification*** – User logon identifiers (“User IDs”) are the most common way of identifying individuals so that the proper access can be granted to them. PIC currently uses the first and middle initials plus the first six or less letters of the user’s last name as the User ID. HUD security policies require that each user have his or her own individual User ID. If you use PIC with someone else’s User ID, this is a security violation! Get your own User ID and use it.
- ***User authentication*** – User authentication refers to the use of passwords or other confirmatory identifiers that prove the User ID is being used by its true owner. PIC currently uses passwords, which must be at least five characters long. PIC management will be increasing the security requirements for passwords in the future. (Later we will describe “good” and “bad” passwords.) Future computer developments in the area of user authentication might involve “biometrics” (such as a fingerprint reader) or the use of “smart cards” (similar to ATM cards) to access HUD systems.

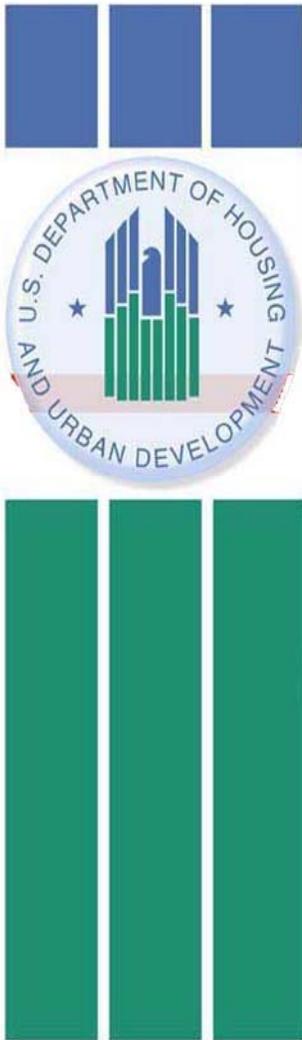


## **Security plans and procedures**

Every business organization should have a written systems security plan and a system disaster recovery plan. These are just as important as fire and police protection to the survivability of the organization.

The security plan must cover the topics covered here as a minimum and assign responsibility for carrying out the policies and procedures. The disaster recovery plan likewise identifies who has what responsibilities in a system disaster and provides the checklists and procedures to accomplish the recovery with greatest efficiency and least losses.

Security procedures cover who may authorize access and how it is done. It might also require employees to sign a Non-disclosure Agreement regarding any data they may handle that is covered by the Privacy Act. It will include procedures to check in and set up new employees and to check out and remove departing employees from access to systems. Normally, system access is removed as soon as management knows an employee will be leaving, not after he or she has left. This reduces the risk of the departing person taking liberties with data or doing damage once they know they are leaving. The security policy will include periodic review of system access to ensure the setup is both current and limited to those with a need for the access. This should be done at least annually. As duties change, it is common to "add" new system access without removing the previous access. This is a bad business practice and can cause unforeseen problems.



## **Good Security Practices**

The information in HUD systems such as PIC is both valuable information and information that must be protected. Failure to take this responsibility seriously is grounds for disciplinary action. There are many good security practices that have been developed by harsh experience in the information technology business over the years. Here is a summary of several of them.

**Passwords Dos and Don'ts.** (Password cracking programs have become very sophisticated. With limited information about you, such as your name and what language you speak, they can guess an old style password in a few minutes. They do this by trying all of the obvious possibilities very quickly, thousands per second). Therefore, passwords should adhere to the following:

- PIC passwords must be 5 and should be at least 8 characters long and are case-sensitive.
- A password should never be an obvious choice such as anyone's name or birth date, pet name, or hobby.
- System administrators should never use the administrator password for anything except system administration. Set up a separate account for everything else, such as timekeeping, e-mail, etc.
- A password should not be a word or phrase normally found in the dictionary (misspell the word intentionally if you must use a word).
- A password should mix letters, symbols and numbers, upper and lower case in a non-standard way.

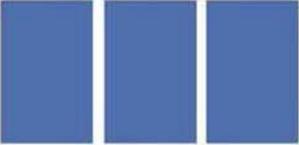
## **Password Examples**

### **"Better" passwords**

&LiBertEE1751  
htiMs72\$Noj&  
64\$%antZY  
186twoCiViLwR  
aNTEEkChARE\$

### **"Worse" passwords**

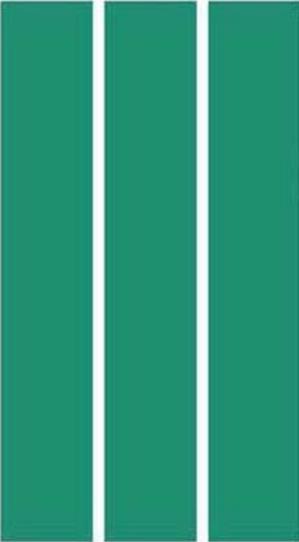
Liberty1776  
JohnSmith  
07041776  
password\$\$  
secrets



## **Good Security Practices (continued)**



Data Backups. Backup media, such as tapes or zip disks, should be kept as securely protected as the original information, which was being backed up. Normally two backup copies are made and one stored outside the building in a secure place. The other one is kept securely nearby. Many organizations use complicated "grandfather-father-son" arrangements of sets of backups but the most important point is to establish a system and schedule and stick to it.



Physical Security. Physical security includes protection of the system hardware, the system access points, the User IDs and passwords, and the media used for data backups. It also includes the paper output of the system which contains sensitive information or working notes, such as screen prints of tenant data and yellow post-in notes with User IDs and/or passwords laying around the desk or thrown in the waste paper basket. User IDs and passwords must be protected by being locked up at all times and/or carried securely on one's person. Preferably, passwords should never be written down, although sometimes that is impractical. Offices should have a paper shredder or separate "confidential" wastebasket, whose contents are regularly burned by confidential staff.

The security plan should be reviewed annually to ensure its relevance. In addition, each user's system access should be reviewed and updated at least annually. Access granted should be documented and filed in the security administration files.

As information technology becomes a larger part of our business, security reviews will become a part of future field reviews. Good security practices are an investment and show a commitment to quality, accuracy and good stewardship of the information collected.



# PIC ANNOUNCEMENTS

---

## I. Release 4.1

- The release of 4.1 is targeted for early May.
- Bob Harmon needs 10-12 testers and will allow for 20 participants.
- This release will include over (50) items that cover many areas. (watch for the detailed announcement soon)

## II. User Acceptance Testing

- PIH Management wants to involve Field personnel and Housing Authorities in the user acceptance testing.
- PIC Coaches are encouraged to send Bob an email if they are interested or if they know of a PHA that might be able to participate.
- This process needs to be performed on a regular and ongoing basis before a release is made available.
- PIC Coaches as well as Housing Authorities are needed for volunteer purposes in order to test the new releases. This will allow the building a better product.
- Bob wants to involve PHA's and HUD staff on the Change Control Board level. This means participating in conference call meetings with the Board to discuss new releases, user acceptance testing, and training issues.

**Please submit comments/suggestions regarding content and format to:**

- Bob Harmon, IT Operations Manager, HUD  
Email: [robert\\_harmon@hud.gov](mailto:robert_harmon@hud.gov)
- Niambi Jarvis-McKnight, Sr. Project Manager, MSSSI (PICHelp)  
Email: [njarvis@mssi2000.com](mailto:njarvis@mssi2000.com)
- Tiffani Jones-Anderson, Project Coordinator/Meetings Facilitator, MSSSI (PICHelp)  
Email: [tjones@mssi2000.com](mailto:tjones@mssi2000.com) or [tiffani\\_j\\_anderson@hud.gov](mailto:tiffani_j_anderson@hud.gov)