Log Out

NeighborhoodInfo DC - Data Warehouse Procedures Guide

Data Security

NeighborhoodInfo DC Data Security Guidelines

Overview and Definitions

All procedures and policies presented here can be superseded by requirements imposed by external agencies regarding confidential data. Please consult with the Data Warehouse Director to determine special requirements for particular data sets.

Overall Guidelines

The Data Warehouse Director, Peter A. Tatian, shall serve as "data security officer" responsible for enforcing the guidelines set forth in this document. All persons with access to the NeighborhoodInfo DC data must sign confidentiality pledges asserting that they will adhere to the guidelines for confidential data use and nondisclosure. All staff are encouraged to restrict use of confidential files as much as possible. Access restriction can be achieved by limiting the use of confidential variables -for example, if a file is considered confidential because it contains identifying names and addresses, those variables may be removed from the file and replaced with pseudo identifiers. The sanitized file may then be used without need for compliance with confidential data requirements.

Definition of Confidential Data

"Confidential data" refers to the following types of information:

- Information designated confidential by external agencies.
- Information designated as sensitive material by the Urban Institute's Institutional Review Board or NeighborhoodInfo DC.

Confidential data in the NeighborhoodInfo DC data warehouse are identified in the metadata system. The presence of confidentiality restrictions for a particular data set will be identified by the "Restrictions:" field on the main data set page. A value of "Restrictions: Confidential," indicates that confidentiality restrictions apply; "Restrictions: None" indicates that no restrictions apply.

Need to Know

Only those with a documented "need to know" are allowed access to confidential data. Staff members affiliated with a project (including the relevant members of the IT staff) need to sign confidentiality pledges for that project.

Anyone without a documented need to know is not to be allowed any access to confidential data.

System administrators for systems that hold confidential data have "need to know" for the purposes of managing those systems.

Confidential Storage Media

A **confidential storage medium** is any form of computer storage (diskette, tape, hard drive, CD, and so on) that:

- Has held any confidential data at any time.
- Has not been "scrubbed" in an approved manner.

Locking Up Data

NeighborhoodInfo DC staff must secure confidential data at all times. Confidential storage media must be logged and secured in a designated, locked filing cabinet. Staff must never leave work stations containing confidential data unattended without first logging out or locking them.

Appropriate Delivery Mechanisms

The following methods for delivering confidential data to the Urban Institute are appropriate and encouraged:

- **File transfer over secure electronic connections.** This means the source system must be a trusted and recognized source for the data (e. g., not a home computer system), and the means of transfer must be secure (such as an encrypted Internet session or a direct dialup connection to the Urban Institute).
- **Certified mail, return receipt requested**, for sensitive data and **Registered mail** for very sensitive data.
- **Hand delivery by a cleared individual.** "Cleared individual" refers to project team members who are authorized to handle the data and who have signed data confidentiality pledges.

Inappropriate Delivery Mechanisms

The following methods for delivering confidential data to the Urban Institute are inappropriate:

- Dialup from home computers (Confidential data should not be on home computers.)
- Unencrypted file transfer over the Internet (examples: ftp, transfer via terminal emulator) to any Urban Institute computer.

[Table of Contents]

Staff Responsibilities Regarding Confidential Data

Confidential Password Management

Passwords that give you access to confidential data are themselves confidential data and should be handled as such for all purposes. Specific password guidelines follow:

- Do not share your password with anyone.
- Do not use easily guessed passwords (personal names, project names, pets' names, words found in a dictionary, words from your native language).
- The most effective passwords contain a mix of uppercase and lowercase letters, and at least one number and special character.
- Never select a password that is completely numeric.
- Choose long passwords. Acronyms created from phrases you can remember are a good approach.
- Do not write down your password. Pick a password you can remember instead of one you'd have to write down.
- If you think your password has been compromised, change it immediately and report the situation as soon as possible to the Director of Information Technology.

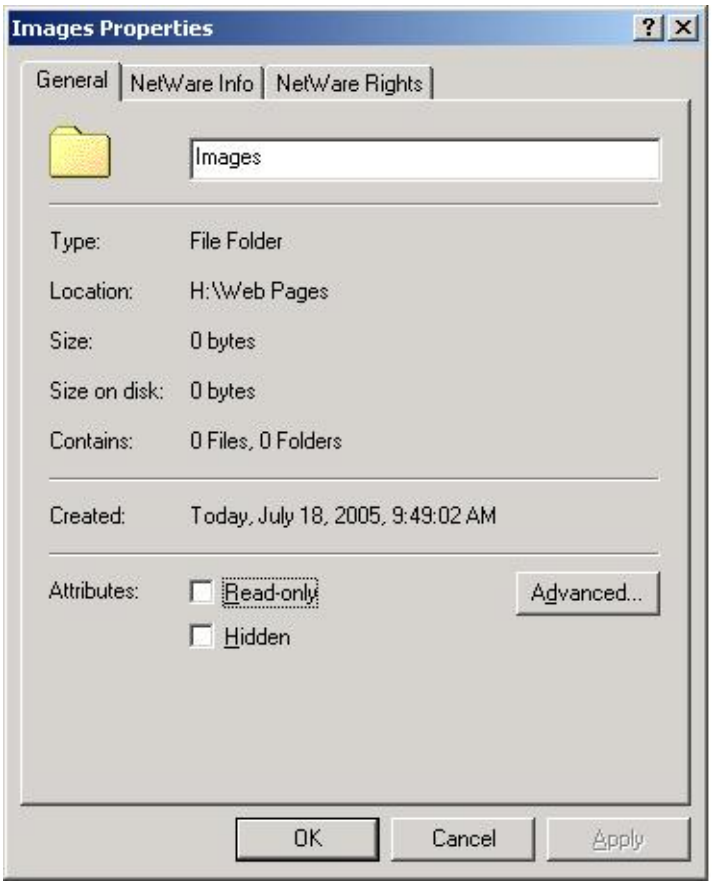
PC Setup

To store confidential data on a PC, you must encrypt the data or use removable storage media that are stored in an approved, locked cabinet. You should encrypt all Windows folders that will hold confidential data, as well as the SAS temporary folder. Instructions are below.

Encrypting Data

Note: Only follow this procedure for folders with data that is confidential.

1. Right click on the folder containing the data you want to encrypt. The following box will pop up.



2. Under the General tab, click on the **"Advanced..."** button. The following box will pop up.

3. Check **"Encrypt contents to secure data"** and then press "OK." The "Advanced..." window will disappear. Press "OK" again on the main Properties/General window. Then the following window will pop up.

4. Select "Apply changes to this folder, subfolders and files" and then press "OK."

Confidential Computer Sessions

- If you are using an account or a computer with access to confidential data, do not leave the session unattended.
- You must log out, and lock up any storage media that hold confidential data.

File Permissions

You may not make confidential data accessible to anyone who is not authorized for that data. Specifically:

On OpenVMS (Alpha 1):
- File protections must deny all access to the World category.
- Access control lists must grant access only to project members. The final entry must deny all access to [*,*I.

On NetWare:
- Access control lists must grant access only to project members and system administrators.

On Windows NT:
- Access control lists must grant access only to project members and system administrators.

Labeling of Confidential Storage Media

You must label storage media (diskettes, tape cartridges, CDs, internal and external hard drives)that hold confidential data with the following information:

- The word "CONFIDENTIAL".
- Tracking number.

Each center is responsible for its own tracking of confidential media.

Logging

You must keep a paper log for each piece of confidential storage media (CD, diskette, tape cartridge, internal or external hard drive)showing what happens to the item while it's in your care.
Log the following events:

- Receipt of item from external source.
- Creation of item at the Urban Institute.
- Destruction of item.
- Transfer of item to someone else's responsibility (even within the Institute).

Each center is responsible for its own logging.

The log should include:

- Date
- Your name
- Description (what happened, to whom transferred, etc.)

Removal of Confidential Storage Media or Printouts

Confidential storage media and printouts can be removed from the Urban Institute only in the following circumstances:

- Hand the item only to a person authorized to receive it.
- Log the transfer.

Printing

Confidential printouts must be stored safely at all times. As a result:

- Do not send confidential data to any of the Institute's "public" printers (where any passerby can see or take the printouts).
- Use printers only if you can be with the printer while it's printing.
- You do not need to log what happens to printouts that never leave the Urban Institute premises.

Disposal or Scrubbing of Confidential Storage Media

The acceptable methods for the disposal or "scrubbing" of confidential storage media are:

- Returning the media to the source.
- Physical destruction by an approved method.
- Erasure using a recommended "secure erasure" product.

Disposal of Confidential Printouts

Dispose of confidential printouts in a shredder, unless externally imposed requirements dictate a different method.

Backups

- Backup tapes, diskettes or CDs containing confidential data must be locked up.
- Backup tapes, diskettes, or CDs containing confidential data must be sanitized before they are discarded or disposed of according to the guidelines in the section on disposal of confidential storage media.

Periodic Review of Confidential Holdings

The Data Warehouse Director will conduct periodic reviews of confidential data handling practices by NeighborhoodInfo DC staff.

[Table of Contents]

Documents to Download

- Staff Assurance of Data Confidentiality
- Confidential Data Log

[Table of Contents]

Date last modified: March 28, 2007
This is an internal-only web site. Please do not distribute the address.