What are Computer Cookies and Temporary Internet files?

- A cookie is a message given to a Web browser by a Web Server. It is stored on your PC and is sent back to the server each time you look at a webpage.
- Cookies are used to identify users and prepare customized web pages for them. When you fill out a form on a webpage with information like your name and interests, the information is made into a cookie and sent to your computer and stored for later use. The next time you go to the same Web site, the cookie will be used to show you a custom Web page. (instead of seeing a generic welcome page you might see a one with your name on it)
- A Temporary Internet File is a file stored on a computer stores the Web site data for every web page that a user visits. They are stored in a file so that the page quickly displays the next time the user visits the same Web site. The browser is opening the Web page from the user's computer instead of downloading the files from the Internet.
- Cookies and Temporary Internet Files can be scanned by hackers, viruses and worms to obtain User ID and Password information.

HMIS System Security

If you are denied services for refusing to give information for HMIS you can call Maine State Housing Authority at 1-800-452-4668 and ask for the Homeless Advocate

What is System Security?

System Security has to do with the Computer System itself. System Security means the steps that we take with the computer system to protect your personal information from people who do not have permission to see or use it.

Why is System Security Important?

System Security is important because your information should only be seen or used by the people you give permission to. If you decide to contribute data or share data, System Security will make sure that no one can gain access to the information in the computer unless a System User gives permission.

What are the Security Measures that HMIS Uses?

- 128 bit Encryption for all data transfers
- Triple DES Encryption (3 levels of Encryption) of Personal Protected Information
- Multiple Level Firewalls
- Public Key Infrastructure (PKI) Technology and/or Device authorization technology
- Hashing (Youth and Domestic Violence Agencies)
- User Authentication
- Secure Websites
- Virus Protection software
- Anti-Spyware software
- Password Protected Computers
- Mandatory regular clearing of cookies and temporary Internet files
- Mandatory regular User Audits and Usage Reviews

What is 128 Bit Encryption?

- 128 Bit Encryption is a way to scramble information and then put it back together. The computer creates a random Key (just like a secret decoder ring) that is used to scramble information. The information is then sent to another computer. The receiving computer receives the key through a different path and uses it to unscramble the information
- Information does not have to be unscrambled on the receiving computer. It can stay encrypted in order to hide personal identifying information.
- 128 bit refers to the amount of space and number of characters used to create the key and the scrambled data.

Not Reviewed or Approved by HUD

What is Triple DES Encryption?

Triple DES is the same as 128 Bit Encryption except that the information is encrypted 3 times. This means that your personal identifying information is encrypted, then that scrambled information is encrypted again, and then that scrambled information is encrypted again. In order to unscramble the information, the User's computer would have to know all 3 keys.

What is a firewall?

A firewall is a way to prevent unauthorized access to or from a private network. A firewall can be on a network or an individual PC. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

What is PKI?

PKI means *public key infrastructure*. It is a system of digital certificates, certificate authorities, and other registration authorities that verify and authorize each person or PC involved in an Internet transaction.

What is Hashing?

Hashing means producing *hash values* for accessing data or for security. A hash value is a number generated from a string of text. The hash is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

What is User Authentication?

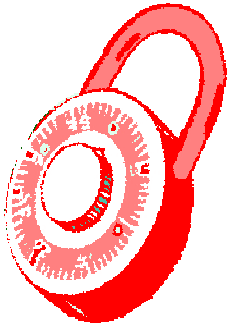
A User is a person who uses a computer. Authentication is the process for authorizing the person to use a specific computer program. Having to enter a User ID and password in order to get access to a computer program is called User Authentication.

What is Secure Websites (SSL)?

Short for *Secure Sockets Layer*, SSL is a protocol for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and the HMIS and ServicePoint Websites use the protocol to obtain confidential user information, such as client identifying information. Webpage addresses that use an SSL connection start with *https:* instead of *http*: for instance https://hmis.maine.gov .

What is Virus Protection?

- A Virus is a program or piece of programming code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus can make a copy of itself over and over again. Even a simple virus is dangerous because it will quickly use all available memory and bring your system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.
- Virus Protection is a program or piece of programming code that runs on your PC and Networks to look for email messages, files, or web pages that contain viruses and prevents the virus from placing itself on your computer or network. An example of a Virus Protection Program is *Norton AntiVirus*.



What are Password Protected Computers?

A Password Protected Computer is a PC that you must sign onto using a User ID and password. You can adjust the amount of time your PC can be idle (unused) before it hibernates. When you want to get back into your computer, you will need to re-enter your User ID and password.

What is Anti-Spyware?

- Spyware is any software that secretly gathers user information through the user's Internet connection without his or her knowledge. Spyware is typically hidden in freeware or shareware programs that can be downloaded from the Internet but are more likely to be secretly downloaded from emails, file attachments and web pages. Spyware monitors your activity on the Internet and transmits that information to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.
- Because spyware uses memory and system resources, the applications running in the background can lead to system crashes or general system instability.
- Because spyware is an independent executable program, they have the ability to monitor keystrokes (what you are typing), scan files on your hard drive, snoop other applications, such as chatroom programs or word processors, install other spyware programs, read cookies, change the default web page on your web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party.

Not Reviewed or Approved by HUD