



Information Technology/ Management of Information System Plan

History:

In 2003, Regis House, Inc. proposed and received a grant from the Health Foundation of South Florida to pursue national accreditation. A major component of the project entailed the implementation of an agency wide data management system to assist in collecting, tracking, and analyzing data on clinical operations. However, it was determined, after extensive research that Knight Integrated Software (KISS) met the agencies needs in terms of components. (See software analysis attached) However, before the software could be purchased and implemented Regis House, Inc. identified significant IT needs that were deemed necessary to support the software conversion. A subsequent grant proposal to the Health Foundation of South Florida in 2004 specifically for technology needs was approved and Regis House, Inc. upgraded its IT system to secure progress toward the goal of achieving national accreditation.

Regis House, Inc. secured the Services of an IT consultant and since then has been able to make the following improvements to the organizations technology system.

HARDWARE:

SERVER: Regis House, Inc. needed to replace our current server with one that has a redundant hard drive (RAID 1) and backup tape/DVD drive, so that we can ensure that all critical and secondary files be stored and backed up there on a regular basis. This will enable us to comply with regulations regarding privacy of client information.

WORK STATION COMPUTERS: Regis House, Inc. needed to replace the computers at seven direct-care staff workstations; the current computers have insufficient hardware and operating systems that necessary to support software used to support clinical software for client records.

WORK STATION PRINTERS: Regis House, Inc. replaced numerous desktop printers being used at workstations for direct-care staff members. These printers, while inexpensive to purchase, rely on a costly ink replacement system. Our IT consultant recommended that it would be more cost-effective to purchase two high-capacity networking printers, with a lower-price ink replacement system, that can be shared by a larger number of staff members.

LAPTOP COMPUTERS: Four laptops were provided to staff that provide community based/on-site services, so that they have a means to enter client data. In addition, key administrative staff were also provided with laptops to increase the off site accessibility and remote access to data.



Information Technology/ Management of Information System Plan

(The annual hardware inventory is attached.)

Security and Confidentiality:

In February 2005 the IT vendor PICT conducted a Technology Security Audit and a report was prepared based on the findings of an on-site audit conducted by PICT on several visits during February 2005. This audit encompassed Regis House, Inc.'s main office and deals only with this location. This document was prepared to provide a summary of Regis House, Inc.'s computing and operating environments, policies and procedures, and to provide recommendations related to compliance with the HIPAA legislation. For more details about the specifics of Regis House, Inc.'s technology environment, please see the PICT document "REGIS HOUSE: Technology Audit", July 2004. (See updated Technology Security Audit, 2010-11).

On May 25, 2005, Regis House, Inc. held a training session facilitated by the IT consultant PICT on viruses because of an agency wide contamination, which nearly ceased operations for days. As a result, the following became part of the IT plan.

Viruses & Spyware

Purpose

This document is provided to PICT clients as a quick reference and policy guideline for general internet security. The recommendations made herein are related to email and internet usage and do not replace or supersede physical network security precautions (such as firewall and antivirus software) or more formal computer usage policies.

Overview

There are several types of security threats facing internet users. These threats can cause loss of data, interruption of service, damage to computers and networks, impairment of computer performance, and lots of wasted time and frustration. Three of the four main threats listed below can be reduced based on user behavior:

- 1. Email Viruses*
- 2. Web Viruses*
- 3. SpyWare*
- 4. Worms*

With the exception of Worms, all of the above threats can be reduced or eliminated through careful use of the internet. In the following sections, we will describe each threat and the precautions, which can prevent infection.



Information Technology/ Management of Information System Plan

E-mail Viruses

Email viruses are common on the internet and range in severity from mild to very destructive. Like all viruses, they are essentially small programs, written to take advantage of a particular security weakness and then spread around the internet. Email viruses take advantage of security weaknesses in email programs like Outlook and the Windows operating system. They are typically spread as attachments to email messages. They can be very sneaky.

The recent Sober virus, once on a computer, reads the Address Book and then begins to send out thousands of new virus attachments to all of the email addresses listed. It disguises the messages to look like a recent email sent or received on the computer, and changes the "From" field to another name on the email list. This fools the receiver into believing that the email came from someone who could be in their circle of acquaintances and the subject and attachment name look like something relevant to him or her. When the receiver opens the attachment, the computer becomes infected and the cycle repeats.

This virus, like most email viruses, generates a huge amount of traffic on the internet and leads many ISPs (Internet Service Providers) to shut down the email servers for infected networks and/or prevent all attachments from moving through their networks. This can create tremendous confusion and inconvenience for millions of people. Infected users may not even realize their computer has been tricked into sending out these viruses because the only outward indication is a slight slowdown.

Other email viruses can be more destructive to the infected computers themselves. Some hijack part of the computer and hard drive to serve pirated software, images, and audio files, others destroy or steal data, still others render the computer unusable.

Prevention:

- 1. Antivirus Software*
- 2. Do not open attachments – Only open an attachment if you are specifically expecting it from the sender.*
- 3. Set Outlook to not download embedded pictures (Go to Tools: Options: Security: Change Automatic Download Settings)*
- 4. Don't use auto respond or away features*
- 5. Set Outlook to notify when a Read Receipt is requested (Go to Tools: Options: Preferences: Email Options: Tracking Options)*



Information Technology/ Management of Information System Plan

Web Viruses & Spyware:

Web viruses and spyware, although different, are generally transmitted the same way so we will cover them together. Both web viruses and spyware are transmitted from web servers to computers using internet browsers. They take advantage of security weaknesses in Internet Explorer (or other browsers), Windows, and user behavior.

Web viruses, once on your computer, can act like email viruses or worms depending on their design and can be mild to very destructive. Spyware is usually less destructive but it can slow down your computer, cause annoying behavior, and provide unknown people with information about your behavior, usernames and passwords, or files on your computer.

Your computer can become infected with these files when you go to a web site or click on a pop-up, which is infected or is intentionally spreading the virus or spyware. When you click on a link in a browser or in an email message, the link does not necessarily go there it says it does.

For example, you may receive an email, which says it is from Citibank, with their logo and official sounding language, asking you to log in and change your password. If it contains a link for you to click on to make the change, it is almost certainly fraudulent, and the link may expose you to a virus or theft. The reason is that anyone can send an email, which looks like it, comes from Citibank, or any other company. The link, which says www.citibank.com/login.asp for example, may actually point to www.joesripoffsite.com/stealmypassword.asp, and you would never know until you receive your bank statement.

Another common method of infection is through pop up windows. If a window pops up while you are browsing offering some incredible deal or informing you that you just won the lottery, it may be a legitimate advertisement or, more likely, an attempt to infect your computer. Most legitimate advertisers avoid using pop-ups, so you should assume that it is dangerous. Most pop-ups offer a button to accept the offer and one to close the window.

EITHER BUTTON WILL INFECT YOUR COMPUTER! Never click on a button or link inside a pop-up window!

Always close them by right clicking on the browser icon on the tool bar at the bottom of your screen.



Information Technology/ Management of Information System Plan

Other common sources of viruses and spyware are downloaded applications and freeware such as music or DVD download sites, screensavers, and browser extensions such as HotBar or YahooBar. Assume that anything being offered for free contains a virus or spyware. Never download and install software from the internet unless your system administrator approves it. Software, which is OK, includes Adobe Acrobat, WinZip, FireFox, and others.

Prevention:

- 1. Antivirus Software*
- 2. Don't click on links in emails unless you are **CERTAIN** that it points to a safe site*
- 3. Close all pop-ups from the tool bar*
- 4. Don't download free software, music players, screensavers, or others*

Worms:

Worms are viruses, which can spread between computers on a network without any user interaction. Once on a computer, they scan the network looking for others and then exploit one or more weaknesses in Windows to spread. They sometimes get onto the first computer as a Web or Email Virus and then spread as a worm. They can be mild to destructive and are often used to attack servers. They always result in slower performance.

Prevention:

- 1. Antivirus Software*
- 2. Firewall*
- 3. Avoiding Email and Web Viruses*

The following is an overview of other IT/MIS items:

Software

MIS Application

Knight Integrated Software

After months of negotiations, on Friday, December 3, 2004, Regis House, Inc. reached an innovative agreement with Spectrum Programs. Spectrum has agreed to lease their client record-keeping and accounting software for a monthly fee that is significantly less than we would invest in purchasing our own license for the software. Spectrum will also provide technical assistance to Regis House, Inc. for the software in terms of establishing



Information Technology/ Management of Information System Plan

access and connectivity, in addition to general technical assistance. Spectrum has already secured approval of this “hybrid license” from the software company KIS in order to introduce their product to a new market segment (smaller agencies) that otherwise would not be able to afford their software. The agreement was executed in March of 2005 and Regis House, Inc. had access the following month.

PICT-Co NewOrg Software

In July 2006 and due to contractual issues the KISS software hybrid operation did not flourish as expected. The new management opted to contract with the current IT/MIS provider and negotiated a software agreement with new software PICT-Co had just developed for non-for-profit organizations.

Regis House, Inc. currently does not have a comprehensive and integrated client and case management solution. Over the past year and a half, Regis House, Inc. has attempted to deploy the KISS case management software hosted by Spectrum. This has not been successful for several reasons including application complexity, limited support from the vendor and Spectrum, staff changes, and organizational changes. Management determined that an application with less focus on financial and insurance billing features and more focus on usability and client management is needed. Moreover, PICT-CO provided significant assistance with the designing and implementing a solution as well as training of the staff. Moving into a web based off-the-shelf application such as the PICT NewOrg will enable the agency with the features to provide the operational benefits desired, and through the ongoing partnership with PICT-CO, provide a more sustainable long term platform.

The following are the areas of interest for the functionality of the NewOrg management software:

1. Create a single Client intake database
2. Schedule and record client sessions and activities
3. Report on staff and department productivity
4. Generate reports for grantors
5. Upload client and service data to grantors to eliminate double data entry
6. Reduce lag time and effort required to generate invoices to grantors

The goals of these improvements are to increase visibility for management throughout the organization, reduce administrative overhead associated with reporting, and improve the accuracy of reporting and billing. We feel that PICT NewOrg software application, combined with ongoing support and assistance from PICT, will meet all of these objectives and also allow the agency to consolidate fundraising, donation management,



Information Technology/ Management of Information System Plan

and HR into a single organizational database system which will be professionally managed and will grow and adapt to the organization's needs.

Below is a list of general functional areas. Many areas are closely integrated with other internal and external areas. The interface is simple and consistent throughout the application with page and field level help screens.

- Client Management
- Client Activity/Services Management
- Scheduling/Group Calendar
- Donor Management
- Donation Tracking
- Event Management
- Staff Productivity Reporting
- Fund & Program Reporting
- Client Services Reporting
- Custom Report Builder
- Import/Export Wizard
- Integration with state and grantor systems
- Integration with MS Exchange

External Functionality

The External section of the Management Center deals with all aspects of communication with external entities and the web site. It allows non-technical users with appropriate permissions to manage the structure and content on the web site from a simple web interface. It also gives users control over many more advanced features such as newsletters, mass emails, event calendars and registration, while integrating with the Internal Management Center for a seamless contact and event management database.

The external or public web interface can be completely customized for each agency based on their existing website design or with a new design integrating their colors, logo, themes, and other display criteria. These sites will not look like standard template driven pages; there is a great deal of design flexibility.

Below is a list of general functional areas. Many areas are closely integrated with other internal and external areas. The interface is simple and consistent throughout the application with page and field level help screens.

- Web site structure and content management
- Newsletters
- Forums



Information Technology/ Management of Information System Plan

- Directories
- Membership forms
- Online Donations
- email Campaign Management
- . Event Registration
- . Calendar

Training

Training is critical to the successful launch of an organization wide information system. PICT provides standard online training materials as well as in depth-help screens and tutorials. PICT will perform an initial general staff training describing the purpose of the system, its functionality, and basic operation. PICT Implementation specialists will then provide one-on-one training in small groups to ensure that each staff member understands how to use the system most effectively for their job function. PICT will provide administrator training to management and a system administrator or staff member designated as a liaison to PICT.

Accounting

QuickBooks

Antivirus

Norton Antivirus

Server O/S

Small Business Server 2003

PICT-Co recommended to upgrade the server to HP 146GB rpm Ultra320 Hot Plug SCSI Hard Drive on 04/15/2009.

On March 3, 2012 a Dell Power Edge T410 Chassis with up to 6 hot-plug hard drives, LCD Diagnostics 12GB Memory server was purchased.

Mail Server

Exchange server 2003

Internal Web Application

To date the South Office cannot access information posted on the internal web site application. In March 2009, PICT-CO recommended the purchase of a Watchguard Firebox x55e with 25 users for the Main location and a Watchguard Firebox with 15



Information Technology/ Management of Information System Plan

users for the South Office to provide accessibility to the internal web posting application to staff, and interns of the South Office.

With the purchase of the new server, the south office will enhance the capabilities of accessing the internal web posting application.

Security

- Individual user names and passwords
- Complex passwords
- Active directory permissions on files and folders
- Administrator account renamed from default
- Guest account renamed and disabled
- Server room locked
- Computers automatically lock after 15 minutes of no activity

Backup Technology

- Off-site out of state encrypted nightly online backups.
- Weekly full backup of server to tape (includes system state, exchange server)
- Shadow Volume Copies enabled

Disaster Recovery

- Weekly full tape backup (includes system state, exchange and all documents)
- Nightly incremental off site backups, stored out of state
- Quarterly ghosted hard drive stored off site.
- Access to email is available off site

Maintenance/Reporting

Implementation of a Troubleshooting Log in October 2005, created the process by which staff, interns and volunteers could report any hardware, software, or IT/MIS issues to the IT Consultants to ensure that access to technology was maintained efficient as a resource.

In 2008, PICT-CO implemented a ticketing system on-line. Staff is able to go on-line and open a ticket for service. Immediately the call is transferred to, the consultant assigned to the agency in his/her blackberry. This mechanism has improved the efficiency of troubleshooting and problem solving. A log is kept of all the tickets opened by Regis House, Inc.'s staff for quality assurance and improvement and trending analyses.

(See Technology Security Audit 2012-15)



Information Technology/ Management of Information System Plan

(See Internal Privacy/Security Audit 2012-15).

(See Management of Information System P&Ps, and Privacy/Security P&Ps).