Recovery Technology

Technology Plan

2019

Recovery Technology

Technology Plan

2019

Information Services Department

Introduction: Recovery Technology is a growing organization in Jackson, Michigan. Recovery Technology's current strategic plan and business operational needs dictate that the information Technology Department keep pace with the organization's current IT configuration and processes as well as detail a plan for the growth of IT capabilities in order to support the organization's strategic plan.

Information Technology Department Description and Policies: Recovery Technology's IT Department is under the direction and supervision of the agency's Chief Executive Officer. The department is comprised of one on site full-time IT specialist. He is responsible for day-to-day operations, administration, application and infrastructure support, and maintaining Recovery Technology's compliance with Health Care Reform Laws and Meaningful Use. He has over 18 years' experience with Information Technology Support and Administration. He has a BBA in Management Information Technology. This Specialist is required to support the full scope of IT department functions from hands on desktop support to systems administration and infrastructure support.

Information Confidentiality: Recovery Technology maintains confidential, protected health information regarding its clients, some of which is maintained electronically. Recovery Technology also maintains proprietary business information that must be protected from unauthorized and/or unlawful access. All electronic documents or files containing confidential treatment or administrative information that are created, maintained, modified, updated or copied using a Recovery Technology computer and/or server must be stored in a location that is secure from unauthorized access and/or encrypted.

Confidential information is defined as a) Electronic Protected Health Information (EPHI): electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. Individually identifiable information refers to any coding or descriptive information by which there is a reasonable basis to believe that the information can be used to identify the individual or by which the individual has been identified in the past. This includes but is not limited to: a person's name (including initials), customer number, address (including zip code), nickname by which the person may be called or commonly known, physical description, description of a particular physical and/or behavioral characteristic, condition, or diagnosis; b) any medical and/or behavioral health information that may be maintained by the company regarding any of its employees or contract workers is considered EPHI; c) Proprietary Business Information (PBI): Information contained in: employee records, contract information and files, company form data, financial data, strategic planning information, company policies and procedures.

Any electronic transmission of confidential information must be protected against unauthorized or unlawful access during the transmission process. This may be accomplished by the encryption at the security level specified within the HIPAA standards and/or utilization of a standardized electronic transfer format specified within the HIPAA standards. Confidential Electronic Information may not be removed from company property on portable computers or any removable media. Removable media is defined as: any media or device that is not internal to company PC that is capable of storing electronic files and information that can be connected to or inserted into another computer that will allow access to the data stored on that device. This includes but is not limited to: a) Externally attached hard drives, b) unmanaged smart phone, c) CD-R/RW and DVD-R/RW media, d) Flash Memory devices.

All employees and contract workers are granted clearance to view and edit confidential electronic information based upon their job functions within the following matrix:

Job Function	*View Confidential Admin. Info.*	*Edit Confidential Admin Info.*	*Transmit Confidential Admin Info.*	*View Confidential Treatment Info.*	*Edit Confidential Treatment Info.*	*Transmit Confidential Admin. Info.*
IT Department Staff	X	P	X	X		X
Leadership: Program Directors	X	X	X	X	X	X
Leadership: Admin	X	X	X	X		P
CEO	X	X	X	X	X	X
Admin Assistant	X		P	X		P
Non-Leadership Admin	X		P	P		P
Other Support	X			P		

Matrix Key: X = Clearance Granted; P = Clearance Granted with Program Director or COO Approval

Recovery Technology staff/contract workers may not transmit or otherwise remove confidential information from a Recovery Technology Computer and/or server unless: a) it is within the scope of their job function to do so, b) The staff/contract worker has the appropriate clearance level to do so, c) Authorization to do so has been granted by the responsible program director.

Storage: Confidential electronic information that must be saved by employees is to be stored by all users with registered MS Office 365 accounts in One Drive. Documents and files are to be stored in a user's "My Documents" folder on Windows based workstations, which is automatically re-directed to the Corporate One Drive. These folders may only be accessible from password protected User accounts and a secure browser. Employees may not store confidential electronic information in their personal computers local hard drives or non-encrypted local drives. Contract workers may store confidential electronic information in their personal or business computers only after the execution of a) a contract with Recovery Technology which delineates the scope of work which will be performed for recovery Technology and b) a Business Associate Agreement which delineates the contract worker's responsibilities regarding the access, use, storage, and destruction of the confidential electronic information they may obtain in the course of performing the contracted functions.

System Security: All access to electronic records maintained by Recovery Technology is restricted by use of strong passwords. All use of company IT resources on the local area network (LAN) and MS Office 365 OneDrive is secured by use of strong passwords.

Company IT resources include, but are not limited to: a) Company owned Computers, Chromebooks, Smart Phones and all data and files stored on them, b) Company owned Removable Devices and hard drives and all data and files stored on them, c) Networked Public or private folders on the Company Servers and all data and files stored on them and/or Cloud Drives (OneDrive, Google Cloud, etc), d) All email and contact information on the Company Exchange Server and/or transmitted across Company Network Infrastructure, f) All Internet usage via Company Network Infrastructure, g) All Instant Messaging transmitted across Company Network Infrastructure.

All company owned computers or Chromebooks, whether they are logging into domain accounts or local workstation accounts are secured from unauthorized access in the following manner:

A. Computers from which it is possible to access confidential client or business information are located within a secure location, with at least one locking door between the computer's location and public areas of the facility.
B. Computers from which it is possible to access confidential client or business information are configured with the requirement of a strong password upon startup of the PC and also upon exiting the screen saver on a running PC.
C. Remote access to Company IT Resources shall be granted only to registered Domain Users on the discretion of the Information Services Staff. All access will be protected by strong passwords and VPN Technology or secure SSL via browser and MS Office 365.

D. Chromebooks are Secured and Managed with Enterprise Chromebook Administration Console which is continuously updated and automatically protected against Malware, Antivirus, and patched regularly.
E. Windows based workstations and servers are protected by Webroot Antivirus/Antimalware and/or Windows Defender. Definition updates and regular scanning are centrally managed and performed regularly. Managed Microsoft Patching is also implemented and updates/rollouts of critical patches and updates will occur regularly.
F. Managed Content Filtration services are implemented and we continue to monitor and specify anything we wish to block/report on using Cisco Umbrella Services provided by Doberman Technologies, LLC.
G. Managed Network Firewall is in place with 24X7 Monitoring with HIPPA/PCI Compliant cloud management service.
H. In 2018 a Security Risk Assessment was completed and Recovery Technology has implemented the findings and recommendations from this report. We also plan to complete annual SRA's to keep our organization up to date with changing technology and security requirements and HIPPA regulations and Meaningful Use compliance.

While Recovery Technology IT Department personnel seek to provide a reasonable level of privacy to users of company IT resources, all persons utilizing the system/accessing records on the system must be aware that all data or files created or stored on the Recovery Technology system are the intellectual property of Recovery Technology. The single exception to this standard is any and all electronic information concerning clients and their treatment, which is adjunct to their medical record and, therefore, the property of the client him/herself. Electronic information concerning clients and their treatment belongs to the client, however Recovery Technology maintains custody of this information and, therefore, the security standards included in this policy and procedure are in full effect.

Failure to adhere to this policy and procedure, inappropriate use of company IT resources, and/or actions that place the security of Recovery Technology IT resources and/or electronic records may result in: a) Revocation of access privileges, b) Possible disciplinary/contract action up to and including termination of employment/contract.

Inappropriate use of company IT resources include:

A. Access and/or viewing of client records without a need to know for business, payment, or treatment purposes;
B. Access and/or viewing for personal gain
C. Access and/or viewing for reasons that are counter to the best interests of Recovery Technology and/or its clients.

Upon separation of employment/termination of contract with Recovery Technology, the IT Department personnel must be notified immediately to ensure that the individual's access to IT resources is immediately disabled. The IT Department must be notified regardless of the reason for the employee's/contract worker's separation from Recovery Technology. In the event that access to IT resources is not immediately disabled, access to IT resources by a former employee/contractor is unlawful and subject to legal action.

System Backup: All Recovery Technology servers are automatically backed up every weeknight. Backups include: a) system volume information, b) system state data, c) application data, d) exchange mailboxes, e) the content of all user folders. Backups are stored at a secure data center. Key users workstations are also backed up incremental nightly and full backups weekly using Arcserve partnered with Doberman Technologies, LLC.

Disaster Recovery: It is the responsibility of the Information Services Department to implement and maintain the following measures to protect against catastrophic loss of data: redundant backups in more than one location off-site using a mixture of technologies including Azure Backup and Arcserve provided by Doberman Technologies, LLC.

Use of Assistive Technology:

Assistive technology products are designed to provide additional accessibility to individuals who have physical or cognitive difficulties, impairments, and disabilities. When selecting assistive technology products, it is crucial to find products that are compatible with the computer operating system and programs on the particular computer being used.

Below are descriptions of the various types of assistive technology products that are currently available on the market today.

Alternative input devices allow individuals to control their computers through means other than a standard keyboard or pointing device. Examples include:

- Alternative keyboards—featuring larger- or smaller-than-standard keys or keyboards, alternative key configurations, and keyboards for use with one hand.
- Electronic pointing devices—used to control the cursor on the screen without use of hands. Devices used include ultrasound, infrared beams, eye movements, nerve signals, or brain waves.
- Sip-and-puff systems—activated by inhaling or exhaling.
- Wands and sticks—worn on the head, held in the mouth or strapped to the chin and used to press keys on the keyboard

- Joysticks—manipulated by hand, feet, chin, etc. and used to control the cursor on screen.
- Trackballs—movable balls on top of a base that can be used to move the cursor on screen.
- Touch screens—allow direct selection or activation of the computer by touching the screen, making it easier to select an option directly rather than through a mouse movement or keyboard. Touch screens are either built into the computer monitor or can be added onto a computer monitor.

Braille embossers transfer computer generated text into embossed Braille output. Braille translation programs convert text scanned-in or generated via standard word processing programs into Braille, which can be printed on the embosser.

Keyboard filters are typing aids such as word prediction utilities and add-on spelling checkers that reduce the required number of keystrokes. Keyboard filters enable users to quickly access the letters they need and to avoid inadvertently selecting keys they don't want.

Light signaler alerts monitor computer sounds and alert the computer user with light signals. This is useful when a computer user cannot hear computer sounds or is not directly in front of the computer screen. As an example, a light can flash alerting the user when a new e-mail message has arrived or a computer command has completed.

On-screen keyboards provide an image of a standard or modified keyboard on the computer screen that allows the user to select keys with a mouse, touch screen, trackball, joystick, switch, or electronic pointing device. On-screen keyboards often have a scanning option that highlights individual keys that can be selected by the user. On-screen keyboards are helpful for individuals who are not able to use a standard keyboard due to dexterity or mobility difficulties.

Reading tools and learning disabilities programs include software and hardware designed to make text-based materials more accessible for people who have difficulty with reading. Options can include scanning, reformatting, navigating, or speaking text out loud. These programs are helpful for those who have difficulty seeing or manipulating conventional print materials; people who are developing new literacy skills or who are learning English as a foreign language; and people who comprehend better when they hear and see text highlighted simultaneously.

Refreshable Braille displays provide tactile output of information represented on the computer screen. A Braille "cell" is composed of a series of dots. The pattern of the dots and various combinations of the cells are used in place of letters. Refreshable Braille displays mechanically lift small rounded plastic or metal pins as needed to form Braille characters. The user reads the

Braille letters with his or her fingers, and then, after a line is read, can refresh the display to read the next line.

Screen enlargers, or screen magnifiers, work like a magnifying glass for the computer by enlarging a portion of the screen which can increase legibility and make it easier to see items on the computer. Some screen enlargers allow a person to zoom in and out on a particular area of the screen.

Screen readers are used to verbalize, or "speak," everything on the screen including text, graphics, control buttons, and menus into a computerized voice that is spoken aloud. In essence, a screen reader transforms a graphic user interface (GUI) into an audio interface. Screen readers are essential for computer users who are blind.

Speech recognition or voice recognition programs, allow people to give commands and enter data using their voices rather than a mouse or keyboard. Voice recognition systems use a microphone attached to the computer, which can be used to create text documents such as letters or e-mail messages, browse the Internet, and navigate among applications and menus by voice.

Text-to-Speech (TTS) or speech synthesizers receive information going to the screen in the form of letters, numbers, and punctuation marks, and then "speak" it out loud in a computerized voice. Using speech synthesizers allows computer users who are blind or who have learning difficulties to hear what they are typing and also provide a spoken voice for individuals who cannot communicate orally, but can communicate their thoughts through typing.

Talking and large-print word processors are software programs that use speech synthesizers to provide auditory feedback of what is typed. Large-print word processors allow the user to view everything in large text without added screen enlargement.

TTY/TDD conversion modems are connected between computers and telephones to allow an individual to type a message on a computer and send it to a TTY/TDD telephone or other Baudot equipped device.

Recovery Technology remains committed to providing services to clients and guests with disabilities, as well as staff with special needs. Recovery Technology will remain current on what is available and the feasibility of utilizing this technology with our clients.

Summary of Current Technology and Spending: When the Information Services Department was started; Recovery Technology had a small handful of Desktop Computers. Currently we have expanded to laptop computers for all case managers and other clinical staff. These computers must be refreshed every four years to prevent the computers from falling into a

state of disrepair causing downtime for the employee and losing productivity and dollars. We are currently in a PC refresh cycle replacing most Case Manager laptops with Chromebooks. The Chromebooks are priced very affordably, meet our user's needs, and are managed and secured easily.

As a startup company, it was sensible for Recovery Technology to spend very conservatively on its Information Technology needs. However, as growth continues, it has become imperative that we focus our attention on a number of areas listed below that will be critical toward achieving and sustaining our Strategic Plan and growth.

1. Computer Hardware: Recovery Technology will continue to purchase Chromebooks for Case Management staff to access the Electronic Medical Record and MS Office 365. We are also refreshing older laptops 4+ years old still in use and any Windows Workstations required by eHR Thomas that cannot be replaced with Chromebooks (local Windows installation).
2. Software and Licensing: As we move to acquire new Computer Hardware, we will be buying computers that come with more up-to-date and Profession versions of Windows 10 OS software or linking staff to Recovery Technology's cloud base services.
3. Network Infrastructure: LAN with high-speed internet connection, seven wireless access points, three primary network printers and supporting equipment have been implemented and upgrades are scheduled this year to optimize network speed and access. New wireless access points and upgrades will be implemented.
4. Disaster Recovery: Experience has revealed that the most common threat we face on a daily basis is the loss of our connectivity to the Internet. When we lose access to the Internet and to LEO, e-mail, etc., this leaves us "dead in the water" and severely impacts our ability to function. This results in a very unfavorable situation for our staff and our clients. We will be investigating a bonding network appliance with packet level load balancing, WAN aggregation and internet failover technology. We will also look at segmenting our wireless network and improving access and reliability throughout the building.

Electronic Medical Record Implementation:

eHR Thomas, from Genius Solutions, has been implemented the first quarter of 2019. We are fine tuning our installation with Genius solutions and reviewing and training staff to e-prescribe, and run reporting for Meaningful Use, and MIPS.

LifeWays CMH, whom Recovery Technology contracts with to provide an array of services, implemented "LifeWay's Electronic Organizer" or LEO. At this time, LEO is fully functioning. Authorization for services and billing are currently being completed in LEO.