

Recovery Technology

Information Technology Plan and Report

2024

Information Services Department

Introduction: Recovery Technology is a mental health clinic 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 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. 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 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), a 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 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 encrypting 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 the company PC that can store 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 smartphones, c) CD-R/RW and DVD-R/RW media, d) Flash Memory devices.

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

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 or by using the Recovery Technology One Drive Shortcut. 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.

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

Company IT resources include but are not limited to: a) Company owned Computers, 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 Drive, 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 using MS Teams, Skype, etc.

All company-owned computers, whether they are logging into Windows Server 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 upon exiting the screen saver on a running PC.
- C. Remote access to Company IT Resources shall be granted only to registered Domain Users at 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. 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.
- E. 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 PC Solutions.
- F. Managed Network Firewall is in place with 24/7 Monitoring with HIPPA/PCI Compliant cloud management service.
- G. In 2023 a Security Risk Assessment was completed, and Recovery Technology is working toward implementing the findings and recommendations from this report.

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 electronic information concerning clients and their treatment, which is adjunct to their medical records and, therefore, the property of the clients themselves. 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 action up to and including termination of employment.

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 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 employees' separation from Recovery Technology. If access to IT resources is not immediately disabled, access to IT resources by a former employee 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.

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.

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 computer being used.

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 that 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 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 four-year PC refresh cycle.

Goals:

As growth continues, we must focus our goals on several 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 Laptop Computers for clinical staff to access the Electronic Medical Record and MS Office 365.

Priority Level: High priority/ongoing

Responsible Staff/Department: IT Administrator, CEO

2. **Software and Licensing:** As we move to acquire new Computer Hardware, we will be buying computers that come with up-to-date and Professional versions of Windows 10 Professional OS software or linking staff to Recovery Technology's cloud-based services and the ability to join an Active Directory Domain.

Priority Level: Medium/ongoing

Responsible Staff/Department: IT Administrator, CEO

3. **Network Infrastructure:** LAN with a 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 and improved.

Priority Level: Low/ongoing

Responsible Staff/Department: IT Administrator/CEO

4. **Disaster Recovery:** Experience has revealed that the most common threat we face daily is the loss of our connectivity to the Internet. When we lose access to the Internet and to Electronic Medical Records, email, 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.

Priority Level: High/ongoing

Responsible staff/Department: IT/CEO

Electronic Medical Record Implementation:

eHR Thomas, from Genius Solutions, was implemented in the first quarter of 2019. We continue to fine-tune our ability to use this system to its fullest capacity. We are continuously adding enhancement requests and preparing new forms to use. This is an ongoing project that requires quarterly review with the leadership team and feedback from the users. Our current Electronic Health Record system continues to meet our needs in 2024.

Lifeways CMH, whom Recovery Technology contracts with to provide an array of services, implemented "Lifeway's Electronic Organizer" or LEO. Currently, LEO is fully functioning. Authorization for services for CMH clients and billing are currently being completed in LEO.

Telehealth: As a result of the COVID-19 pandemic, we were tasked with creating a mobile workforce and providing Telehealth services to our clients. Telehealth continues to assist us in the ability to expand our services and expand access for clients. Groups have continued to be conducted primarily via telehealth. We also use Doxy.me, Secure Video and Microsoft Teams services while leveraging our existing MS Teams enabled workstations and cellular phones which can run all the same software as our laptops/workstations. All of our telehealth solutions are safe and secure, and meet the requirements for HIPPA privacy and MDHHS standards. We will continue to take feedback from clients and employees to improve upon the hardware, software, and processes to provide the best possible services possible.